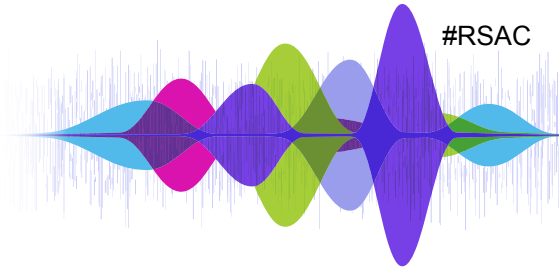
RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: HUM-R06

Making OSINT Education Practical: Why Don't You Go Dox Yourself?

Zoe Lindsey
Security Strategist
Blumira
linkedin.com/in/zoelindsey



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Agenda

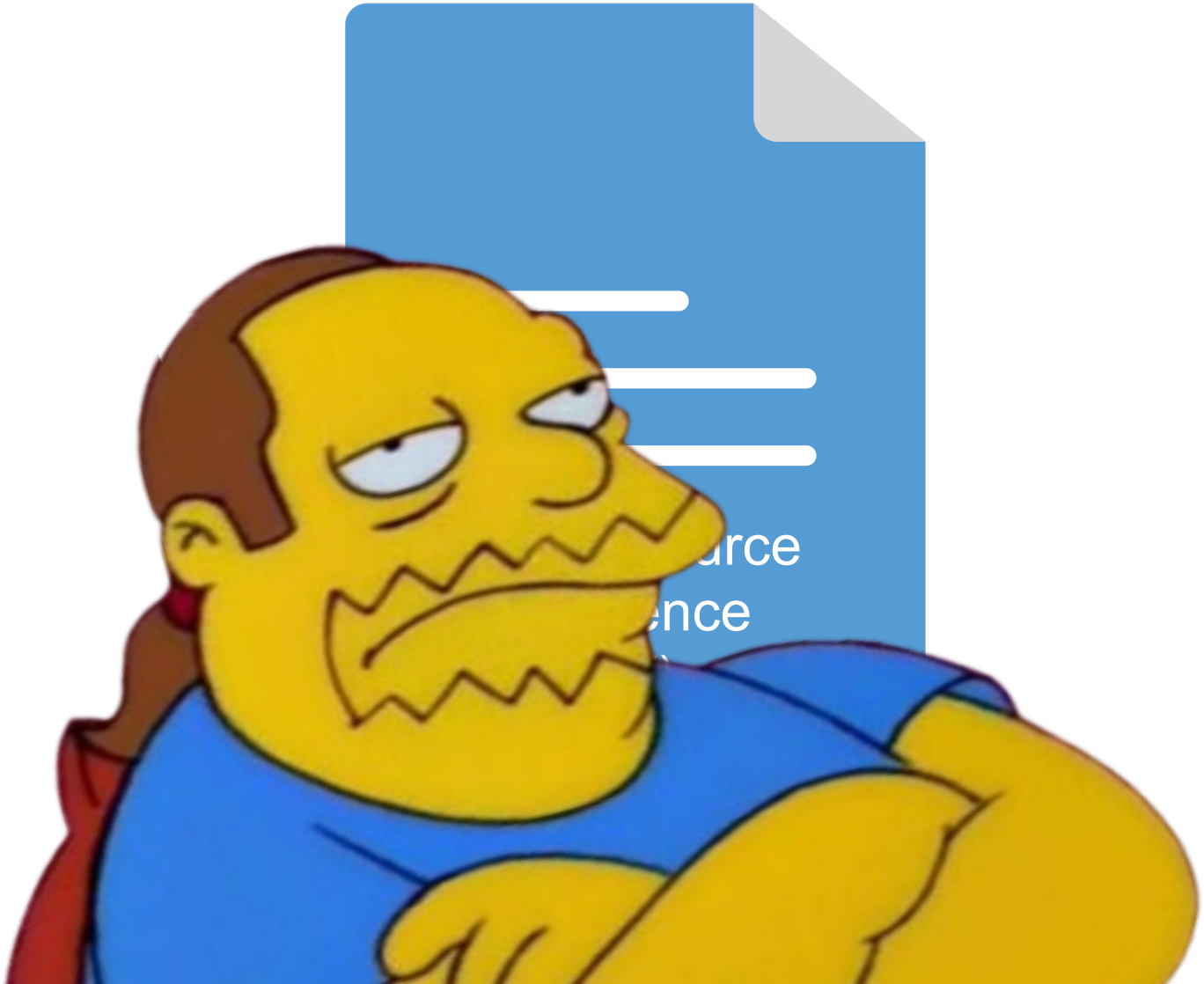
1. What Doxxing Is
2. Who Gets Doxxed, And Why
3. Data Alchemy & The Security Mindset
4. The Process: Recycling the 3 Rs
5. Recap & Supporting Communal Security

What Do You Mean By “Dox”?

What Do You Mean By “Dox”?

What Do You Mean By “Dox”?

What Do You Mean By “Dox”?



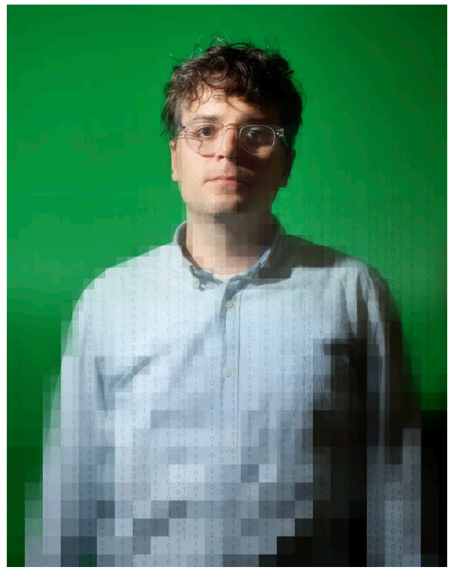
2012: Cascade Failure

How Mat Lost His Apple Account… And Everything Else

MAT HONAN GEAR AUG 6, 2012 8:01 PM

How Apple and Amazon Security Flaws Led to My Epic Hacking

In the space of one hour, my entire digital life was destroyed. First my Google account was taken over, then deleted. Next my Twitter account was compromised, and used as a platform to broadcast racist and homophobic messages. Here's the story of exactly how my hackers created havoc by exploiting Apple and Amazon security flaws.



Meet Mat Honan. He just had his digital life dissolved by hackers. PHOTO: ARIEL ZAMBELICH/WIRED. ILLUSTRATION: ROSS PATTON/WIRED

- Personal site had Gmail address
- Saw m****n@me.com as password reset backup
- WHOIS for billing address
- Used SE to get last 4 of credit card from Amazon

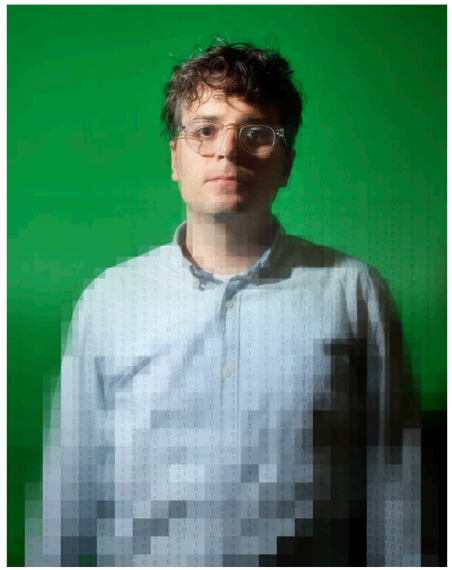
2012: Cascade Failure

How Mat Lost His Apple Account… And Everything Else

MAT HONAN GEAR AUG 6, 2012 8:01 PM

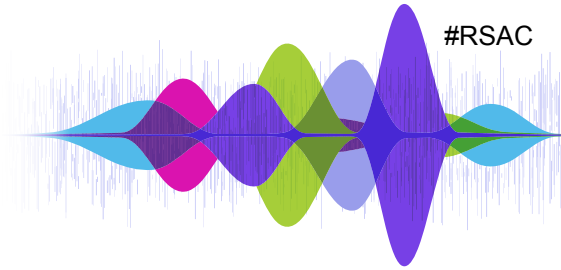
How Apple and Amazon Security Flaws Led to My Epic Hacking

In the space of one hour, my entire digital life was destroyed. First my Google account was taken over, then deleted. Next my Twitter account was compromised, and used as a platform to broadcast racist and homophobic messages. Here's the story of exactly how my hackers created havoc by exploiting Apple and Amazon security flaws.



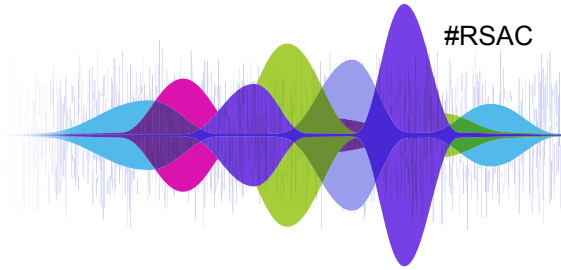
Meet Mat Honan. He just had his digital life dissolved by hackers. PHOTO: ARIEL ZAMBELICH/WIRED. ILLUSTRATION: ROSS PATTON/WIRED

- Used last 4 acquired from Amazon to “verify” Apple ID
- Forced Apple password reset
- Remotely wiped devices to delay discovery/resolution
- Used newly-accessed Apple email to reset Gmail account



"But I'm not a celebrity, executive, or a major journalist! Who's going to want to dox me?"

- Most People, Probably

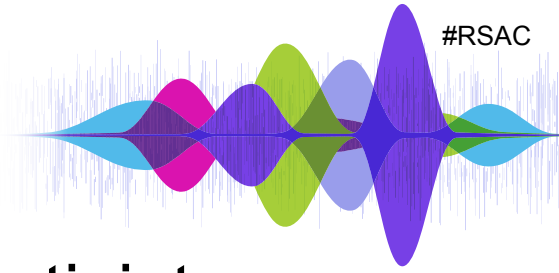


13 Reasons Why People Get Doxxed

- Bullying
- Blackmail
- Domestic Abuse
- Extortion
- Investigation
- Public Humiliation
- Political Pressure
- Sexual Harassment
- Social Engineering Recon
- Stalking
- Swatting
- Whistleblower Retaliation

… and, of course:

- “for the lolz”



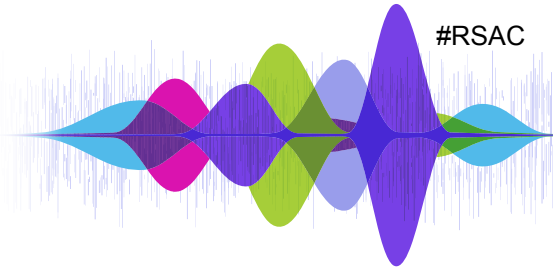
13 Common Targets

- Students
- Public Figures
- Intimate Partners
- Purchasing/Finance Roles
- Social Engineering Targets
- Social Media Posters
- Politicians & Activists
- Government Employees
- Women
- LGBTQ+ People
- Racial Minority Groups
- Journalists

… and, of course:

- “Bad-Luck Bystanders”

The Venn Diagrams Look Even Worse



58%

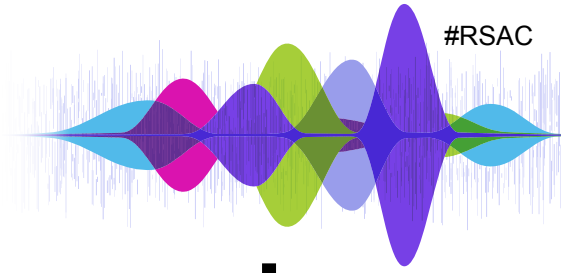
girls and young women who reported online harassment [1]

73%

women journalists have experienced online violence [2]

80%

80% of young LGBTQ+ people of color have reported online harassment [3]

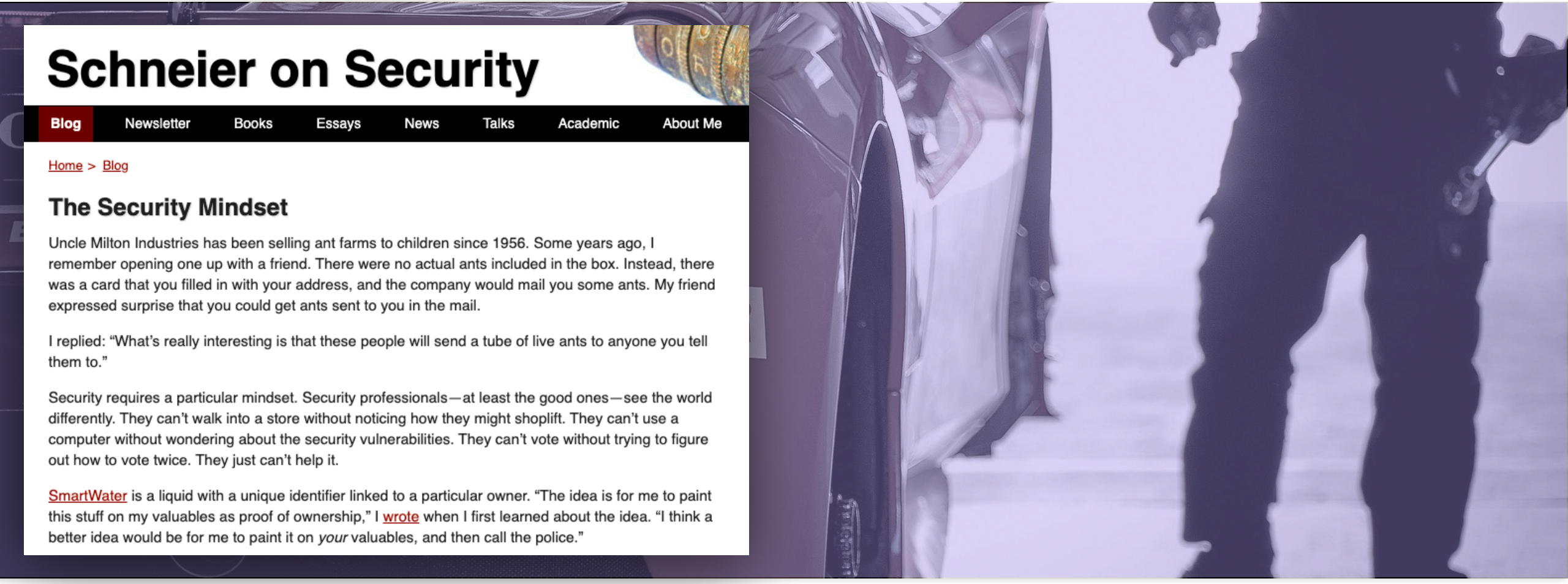


"Ok, sure. But all of this sounds horrible (and even worse, like a lot of work!) So… why would I ever do this to *myself?*"

- Most People, Probably (Again)

Cultivating the Security Mindset

1 Weird Trick For A Free Car: Honest people hate it!



Schneier on Security

Blog | Newsletter | Books | Essays | News | Talks | Academic | About Me

Home > Blog

The Security Mindset

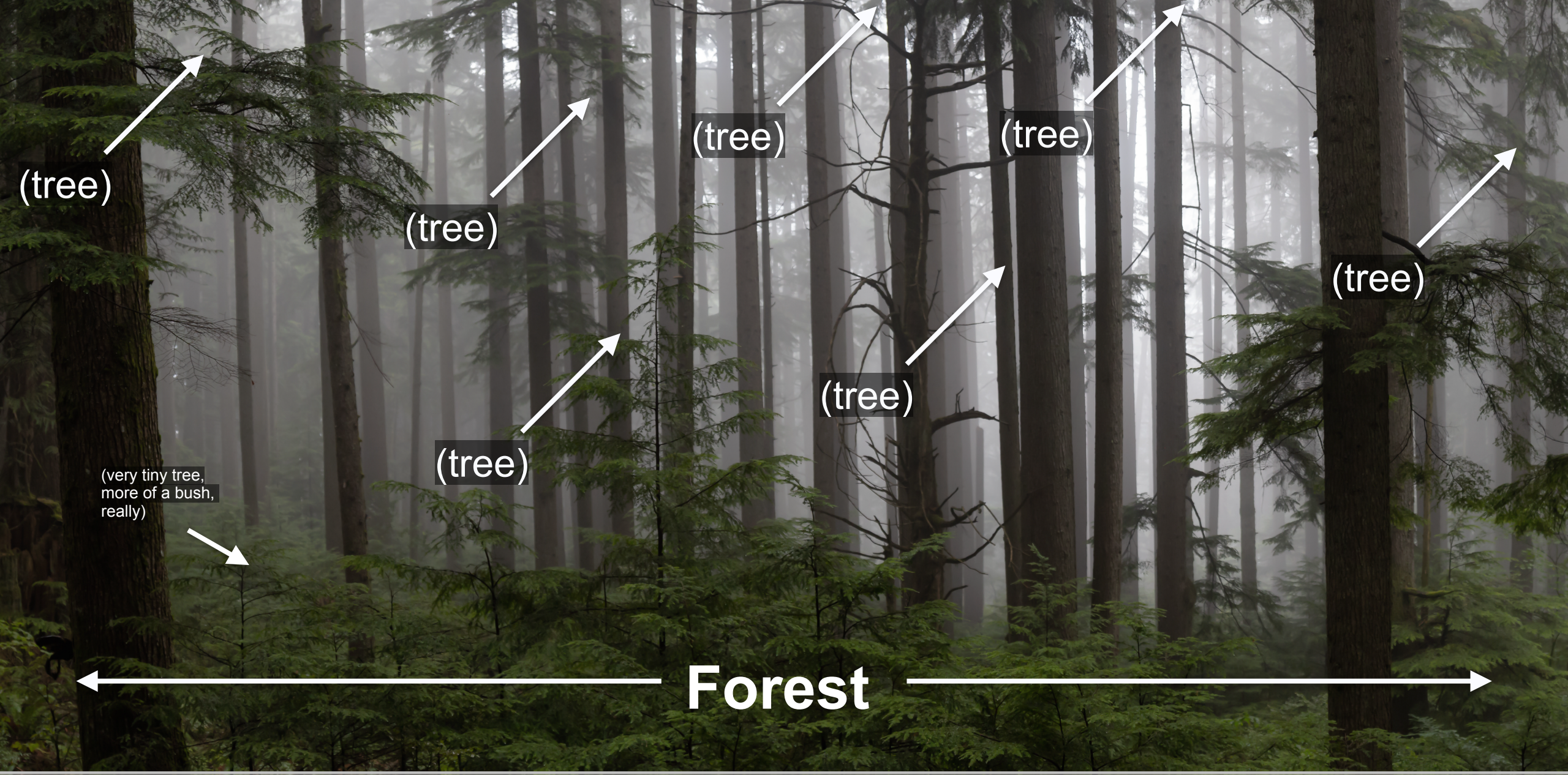
Uncle Milton Industries has been selling ant farms to children since 1956. Some years ago, I remember opening one up with a friend. There were no actual ants included in the box. Instead, there was a card that you filled in with your address, and the company would mail you some ants. My friend expressed surprise that you could get ants sent to you in the mail.

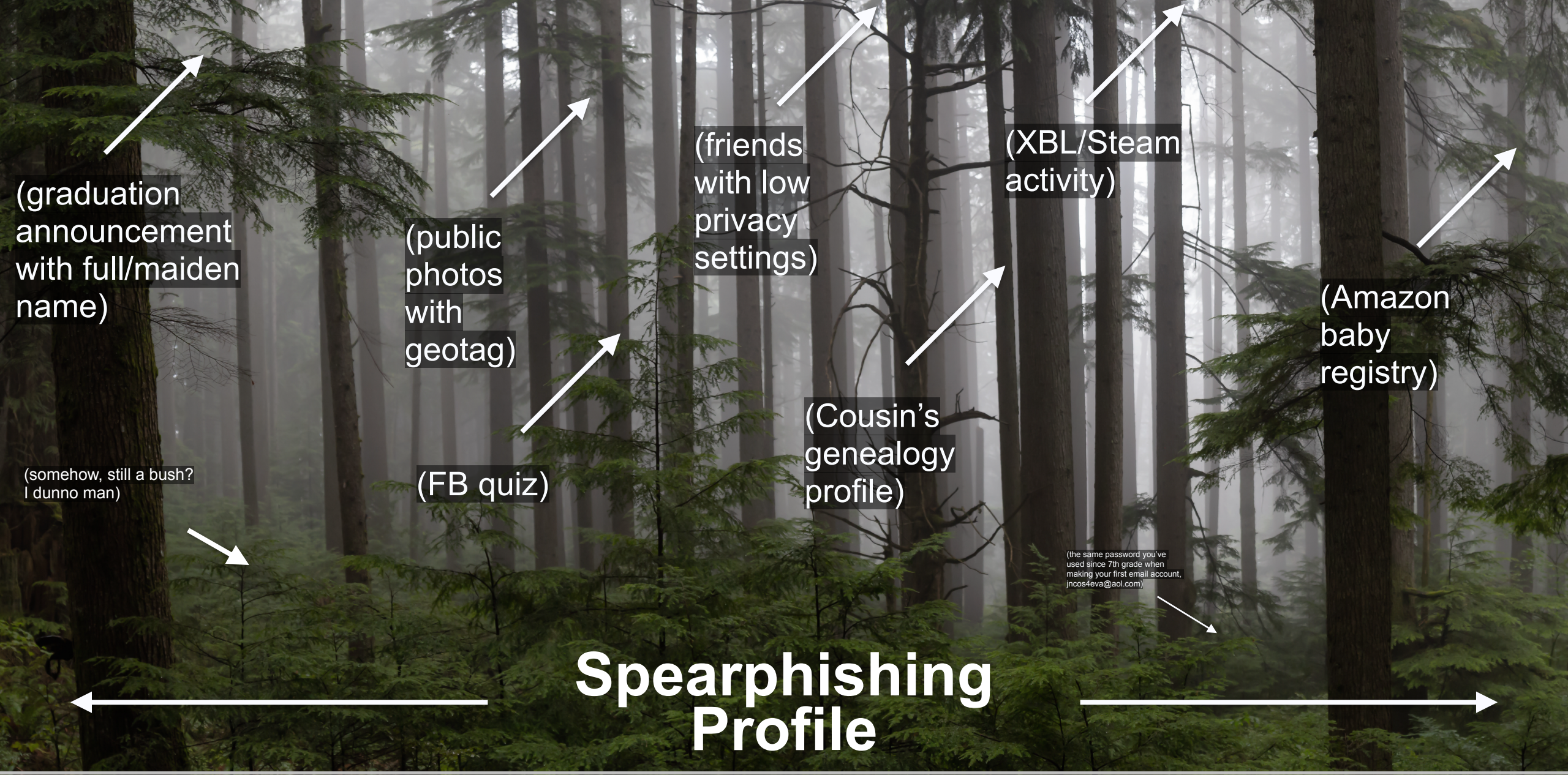
I replied: "What's really interesting is that these people will send a tube of live ants to anyone you tell them to."

Security requires a particular mindset. Security professionals—at least the good ones—see the world differently. They can't walk into a store without noticing how they might shoplift. They can't use a computer without wondering about the security vulnerabilities. They can't vote without trying to figure out how to vote twice. They just can't help it.

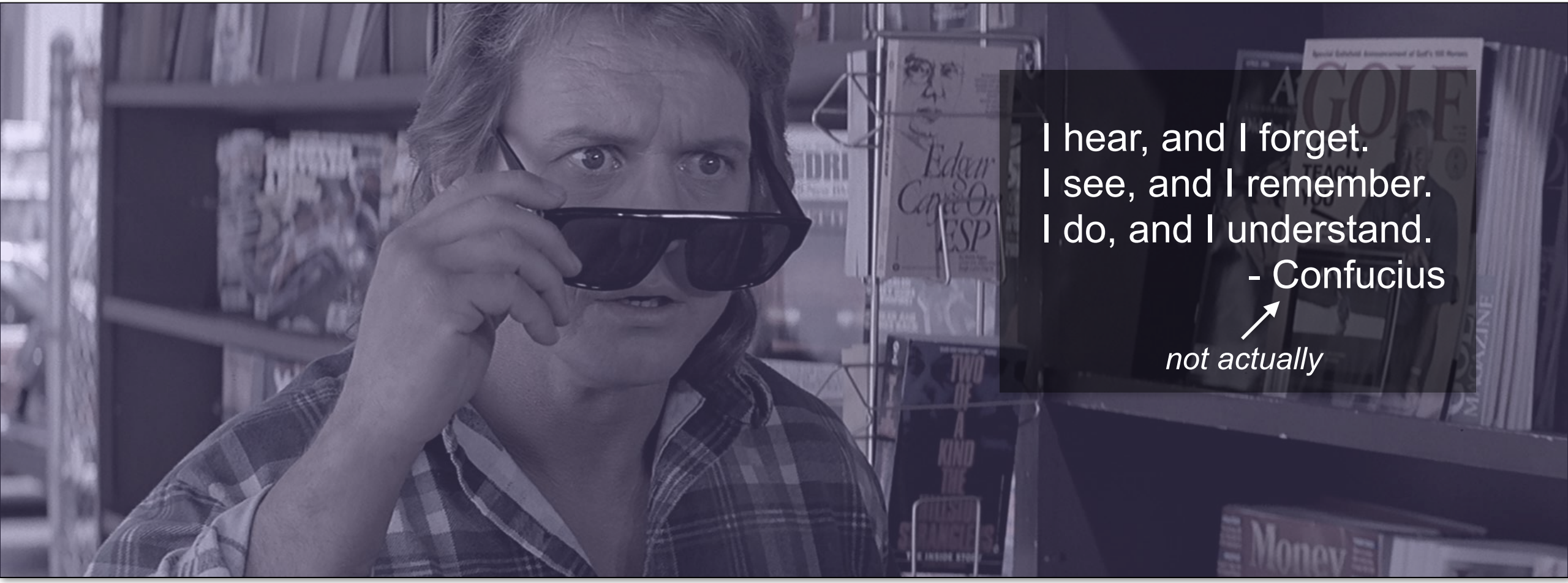
SmartWater is a liquid with a unique identifier linked to a particular owner. "The idea is for me to paint this stuff on my valuables as proof of ownership," I wrote when I first learned about the idea. "I think a better idea would be for me to paint it on *your* valuables, and then call the police."

(tree)


(tree)
(tree)
(tree)
(tree)
(tree)
(tree)
(tree)
(very tiny tree, more of a bush, really)
Forest


(graduation announcement with full/maiden name)
(public photos with geotag)
(friends with low privacy settings)
(XBL/Steam activity)
(Amazon baby registry)
(somehow, still a bush? I dunno man)
(FB quiz)
(Cousin's genealogy profile)
(the same password you've used since 7th grade when making your first email account, jncos4eva@aol.com)
Spearphishing Profile

Reset Your Mindset



Why Reinvent the ~~Wheel~~ Cycle?

REDUCE

RECYCLE

RE-USE

Have A Helpful Acronym!

REVIEW

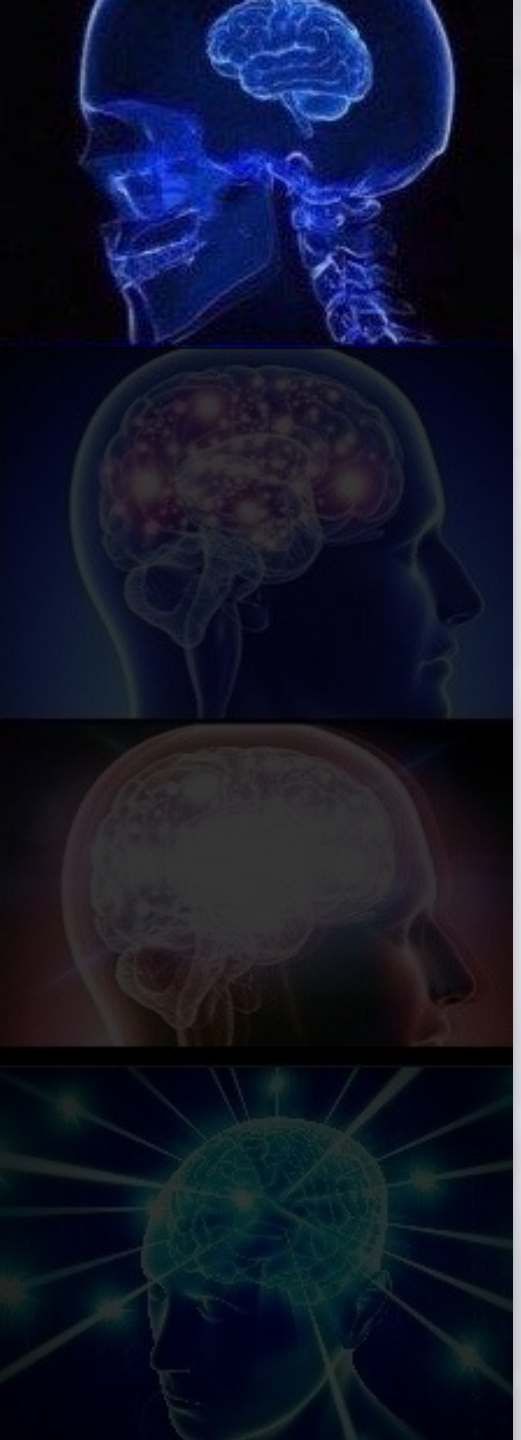
REMOVE

RESTRICT

REVIEW

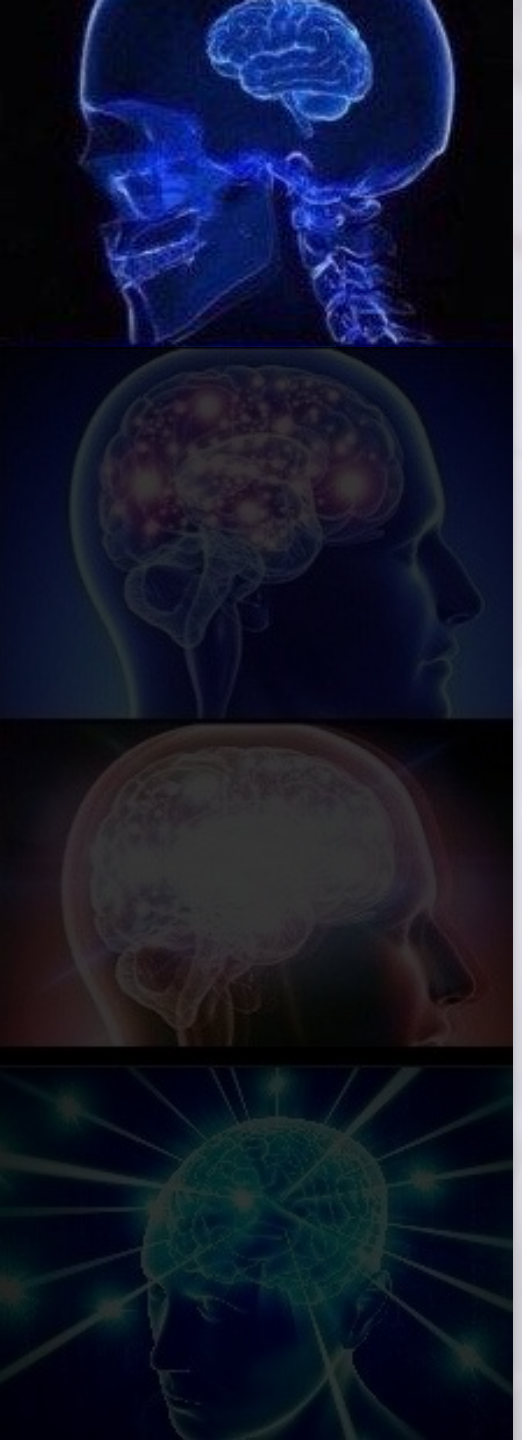
- Account Inventory
- Public Records
- Privacy Settings
- Personal Connections
- Search Results

There's Levels To This S…earch

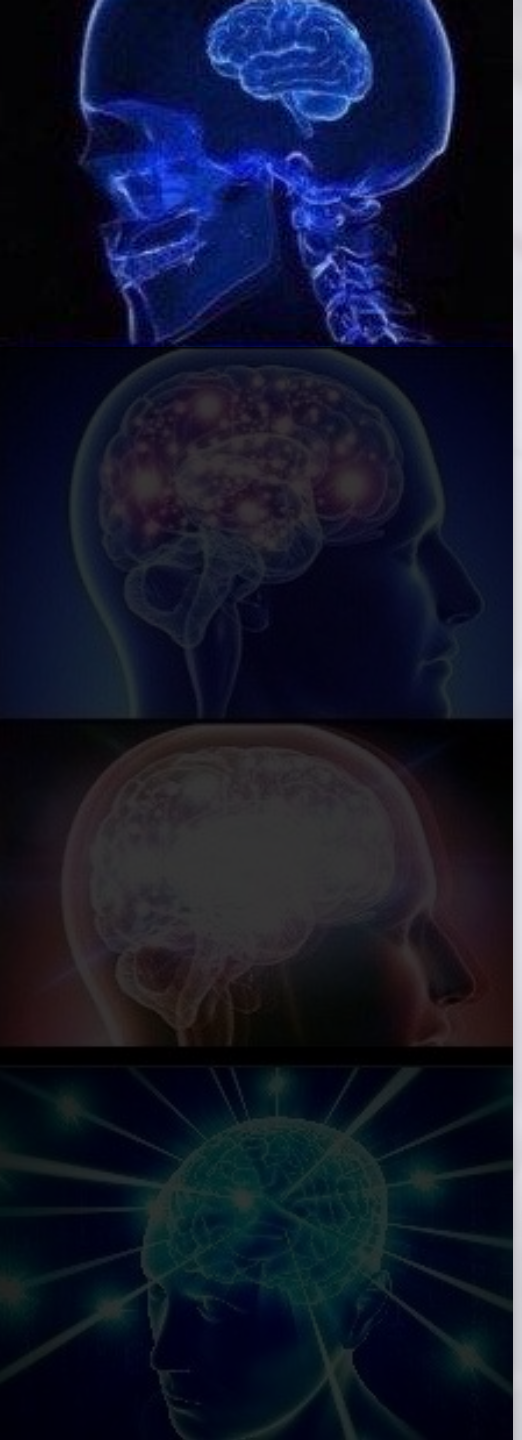


Level One: Basic Info

- Address History
- Phone Number(s)
- Email(s)
- DOB / SSN
- Search Results



“Why am I so obsessed with me?”



sundowndev / GoogleDorking.md

Last active yesterday

Star 1,880 Fork 502

Code Revisions 9 Stars 1,866 Forks 502

Embed <script src="https://

Download ZIP

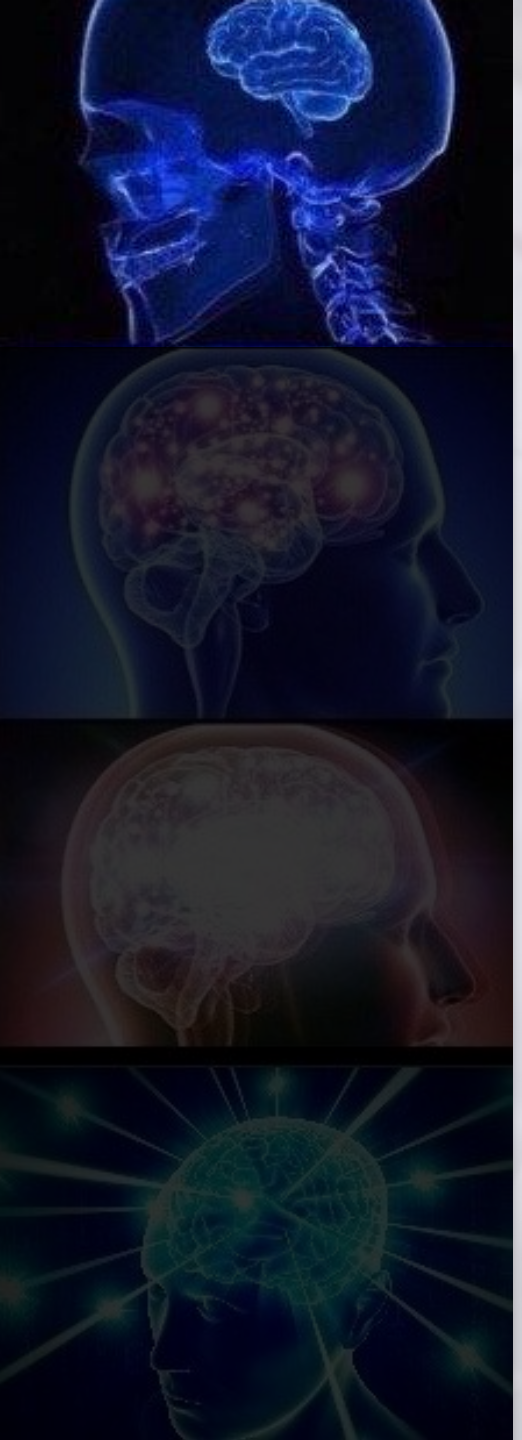
Google dork cheatsheet

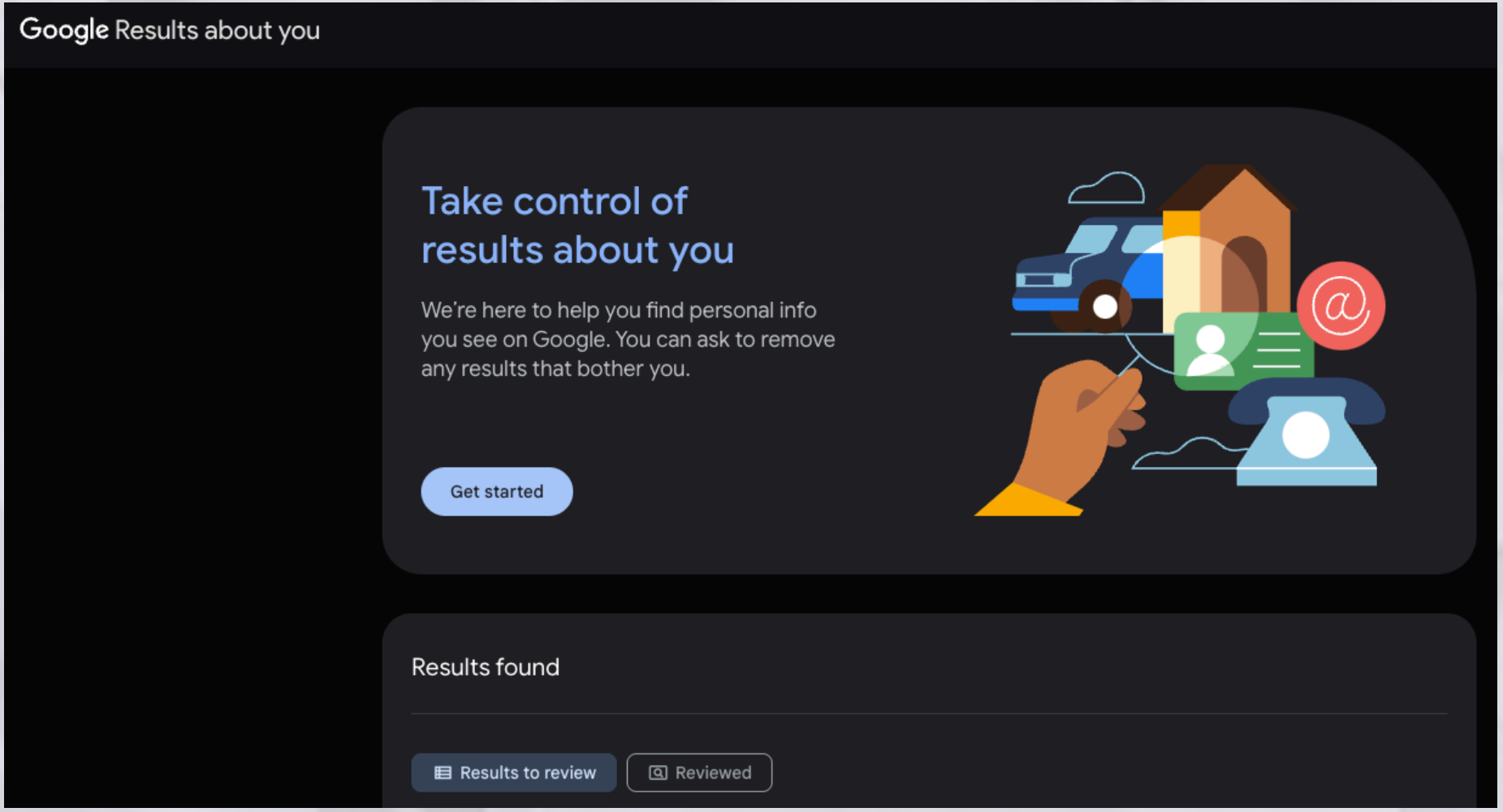
GoogleDorking.md Raw

Google dork cheatsheet

Search filters

Filter	Description	Example
allintext	Searches for occurrences of all the keywords given.	`allintext:"keyword"`
intext	Searches for the occurrences of keywords all at once or one at a time.	`intext:"keyword"`
inurl	Searches for a URL matching one of the keywords.	`inurl:"keyword"`
allinurl	Searches for a URL matching all the keywords in the query.	`allinurl:"keyword"`
intitle	Searches for occurrences of keywords in title all or one.	`intitle:"keyword"`




Google Results about you
Take control of results about you
We're here to help you find personal info you see on Google. You can ask to remove any results that bother you.
Get started
Results found
Results to review
Reviewed

Level Two: Primary Connections

- Family Members
- School History
- Work History
- Social Media Profiles
- Usernames/Accounts

Critical Usernames/ Accounts:

- Financial Accounts
- Electronic Health Records
- Identity Accounts
- Backup/Verification Accounts

Using Facebook › Friending

People You May Know

What is People You May Know on Facebook?

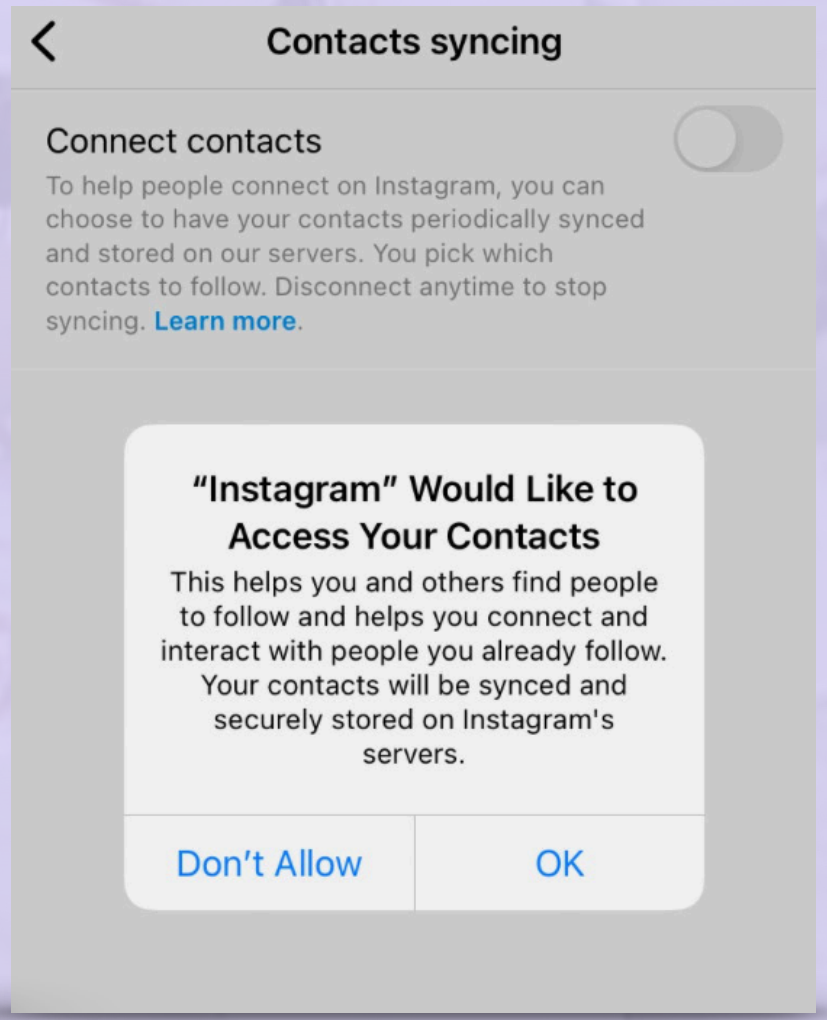
How can I manage information used for People You May Know?

There are different ways you can control what information People You May Know uses.

You can:

- Change the privacy settings of your friends list.
- Limit who can send you friend requests to friends of friends.
- Manage mobile phone and email contacts you uploaded to Facebook or Messenger.
- Control who Facebook can suggest your profile to based on your email address or phone number.

Learn more about what information we collect and how it's used in our Privacy Policy.


Contacts syncing
Connect contacts
To help people connect on Instagram, you can choose to have your contacts periodically synced and stored on our servers. You pick which contacts to follow. Disconnect anytime to stop syncing. Learn more.
"Instagram" Would Like to Access Your Contacts
This helps you and others find people to follow and helps you connect and interact with people you already follow. Your contacts will be synced and securely stored on Instagram's servers.
Don't Allow
OK

Sparks Joy
(restrict)

Doesn't Spark Joy
(restrict)

NordPass

Juggling security: How many passwords does the average person have in 2024?

April 24, 2024 - 5 min read

Kamile Viezelyte

Cybersecurity Content Writer

Search mail

From

To

Subject {confirm activate (verify your email) (forgot password) subscription (reset password)}

Has the words

Doesn't have

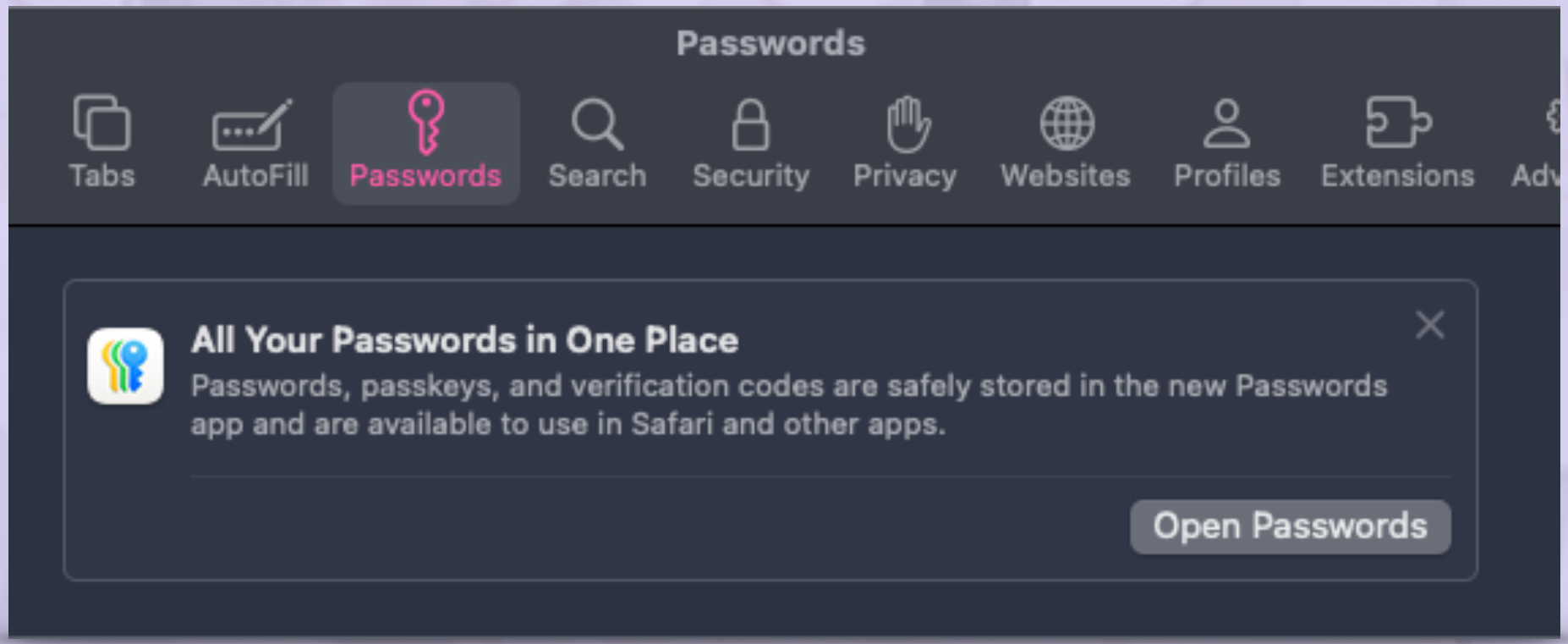
Size greater than MB

Date within 1 day

Search All Mail

Has attachment

Create filter Search


Passwords
Tabs
AutoFill
Passwords
Search
Security
Privacy
Websites
Profiles
Extensions
All Your Passwords in One Place
Passwords, passkeys, and verification codes are safely stored in the new Passwords app and are available to use in Safari and other apps.
Open Passwords

Instant Username Search

this_is_an_example

Social

Instagram	Unknown
~~TikTok~~	Taken
~~X (Twitter)~~	Invalid
~~Facebook~~	Invalid
~~Snapchat~~	Invalid
Reddit	Available
~~Bluesky~~	Invalid

Video

YouTube	Available
~~TikTok~~	Taken
Twitch	Available
Vimeo	Unknown
Rumble	Available
DailyMotion	Available

Professional

~~LinkedIn~~	Invalid
Slack	Available
~~Fiverr~~	Invalid
~~GitHub~~	Invalid
GitLab	Available
HackerNews	Unknown

More

Gaming

SteamGroup	Available
Xbox Gamertag	Available
Minecraft	Available
Lichess	Unknown

Art

Dribbble	Available
Behance	Available
Redbubble	Unknown
ArtStation	Unknown

Blogging

Medium	Available
WordPress	Available
Blogger	Available
~~DeviantART~~	Taken

Level Three: Extended Connections

- Press Mentions
- Political Donations
- Profile Photos
- Domains/IP Addresses
- Property/Legal Records

Google

Google news | Search Archive | Search the Web | Archive Search Help

All Newspapers A B C D E F G H I J K L M N O P Q R S T U V W Y

A

A Propos
164 issues
Sep 16, 1973 - Aug 17, 1974

L'Abeille de la Nouvelle
275 issues
Dec 31, 1862 - Dec 31, 1870

Acadian Recorder
128 issues
Nov 18, 1854 - Dec 28, 1861

L'Action Conservatrice
2 issues
Jun 21, 1935 - Oct 11, 1935

L'Action Québec
534 issues
Nov 1, 1971 - Sep 8, 1973

Adams County News
354 issues
Nov 28, 1908 - Aug 25, 1917

Advertiser-News
11 issues
Oct 6, 1977 - Dec 27, 1979

The Age
32,807 issues

A'tome
23 issues
Feb 14, 1974 - Dec 19, 1974

L'abeille de la Nouvelle-Orleans
14,981 issues
Jan 1, 1846 - Dec 28, 1929

L'Acadien
922 issues
Dec 31, 1819 - Aug 13, 1929

L'Action des Deux Montagnes
70 issues
Oct 4, 1962 - Aug 25, 1965

L'Action Sociale
1,333 issues
May 1, 1903 - Dec 30, 1915

The Adams County Record
110 issues
Dec 1, 2005 - Apr 15, 2009

The Advocate
48 issues
Jan 14, 1886 - Jan 6, 1887

The Age-Sentinel
61 issues

L'Abeille
752 issues
Sep 4, 1827 - Dec 31, 1830

The Aberdeen Times
363 issues
Nov 28, 1968 - Apr 15, 2009

L'Action
23 issues
Jan 3, 1963 - Feb 28, 1963

L'Action Libérale
345 issues
May 3, 1888 - Sep 26, 1931

The Acton Free Press
65 issues
Sep 6, 1894 - Dec 25, 1895

The Advertiser
216 issues
Jul 11, 1868 - Jan 3, 1873

The Afro American
3,623 issues
Jan 4, 1902 - Dec 26, 1992

L'Aide à la France
2 issues

L'Abeille Canadienne
10 issues
Dec 7, 1833 - Feb 8, 1884

L'Abitibi
244 issues
Jan 22, 1920 - Feb 24, 1925

L'Action Catholique
7,461 issues
Dec 31, 1915 - Dec 11, 1962

L'Action Populaire - L'Horizon
2,273 issues
Mar 6, 1913 - Jun 17, 1970

The Adams Centinel
2,142 issues
Nov 19, 1800 - Mar 19, 1883

The Advertiser and Eastern Townships Sentinel
561 issues
Jan 11, 1856 - Nov 7, 1887

The Afro American Ledger
286 issues
Jan 5, 1906 - Jun 30, 1917

L' Aiglon
198 issues

Google
Images
Search any image with Google Lens
Drag an image here or upload a file
OR
Paste image link
Search

PimEyes

Search Pricing Blog Opt-out FAQ Contact

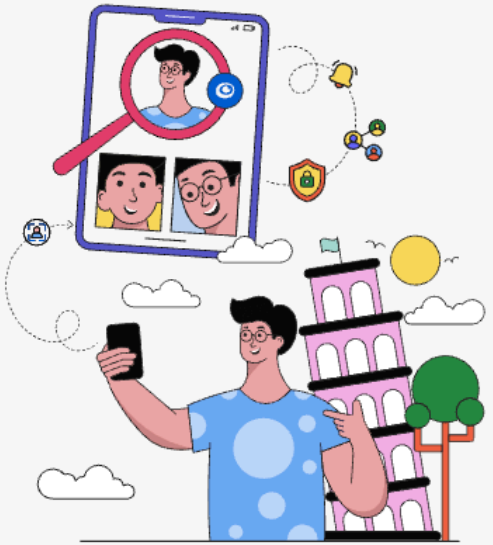
EN

Face Search Engine Reverse Image Search

UPLOAD PHOTO AND FIND OUT WHERE IMAGES ARE PUBLISHED

Upload photo(s)

Or you can take a photo with the device's camera. Don't worry, we will not store it!



„It's quick, it's accurate, it's facial recognition on steroids"

BBC

„PimEyes, a search engine that's handy for reverse image searching and facial recognition."

VICE

„The facial recognition site PimEyes is one of the most capable face-searching tools on the planet."

The Washington Post

„For $29.99 a month PimEyes offers a potentially dangerous superpower from the world of science fiction"

New York Times

Shodan | Maps | Images | Monitor | Developer | More...

SHODAN 8.8.8.8 Login

Mountain View | Portola Valley | Sunnyvale

8.8.8.8

Regular View | Raw Data | Timeline | Satellite © MapTiler © OpenStreetMap

// LAST SEEN: 202

General Information

Hostnames	dns.google
Domains	DNS.GOOGLE
Country	United States
City	Mountain View
Organization	Google LLC
ISP	Google LLC
ASN	AS15169

Open Ports

53 | 443

// 53 / TCP

Recursion: enabled

// 53 / UDP

Recursion: enabled

// 443 / TCP

Google Public DNS

lookup.icann.org/en/lookup

Contact Information

Registrant:

Handle: GOGL

Name: Google LLC

Whois Server: whois.arin.net

Kind: org

Mailing Address: 1600 Amphitheatre Parkway, Mountain View, CA, 94043, United States

Registration comments:

please note that the recommended way to file abuse complaints are located in the following links.

to report abuse and illegal activity: https://www.google.com/contact/

for legal requests: http://support.google.com/legal

regards,
the google team

Abuse:

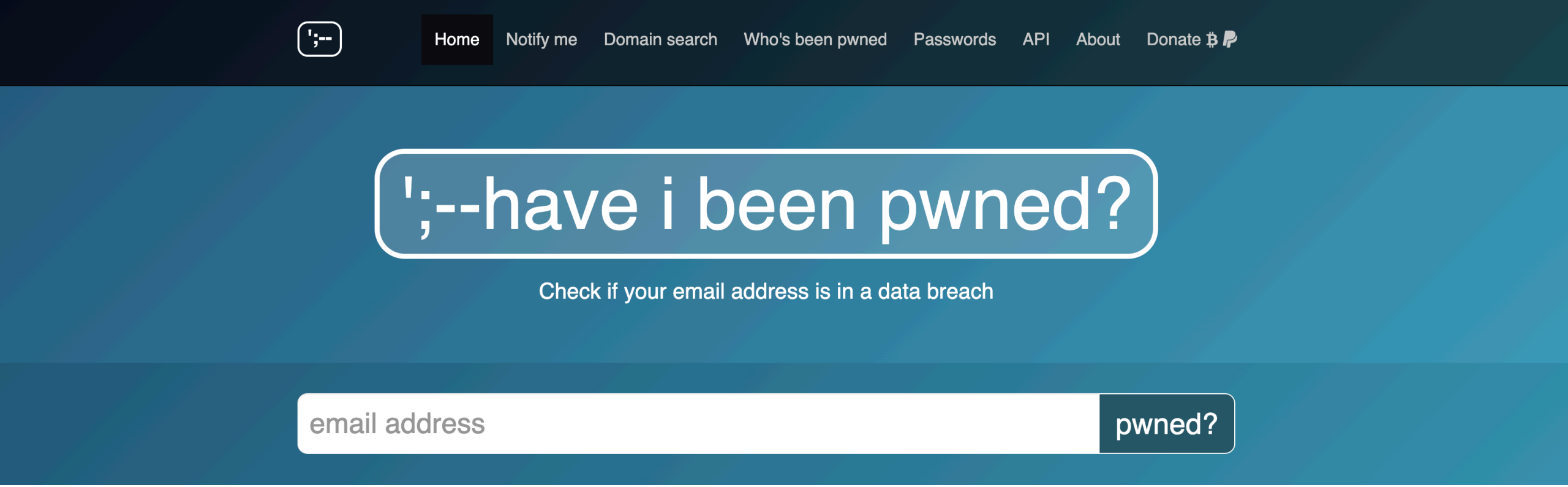
Handle: ABUSE5250-ARIN

Level Four: Targeted Research

- Tracker History
- Search/Browsing History
- Voice/Video Recordings
- Stylometry
- Toilet Paper Orientation

- Improve Login Security
- Third Party App Access
- Separate Email Channels
- Ad Personalization/Tracking
- Privacy Settings
- Credit Bureau Freeze

RESTRICT



... yeah, probably.

They will, they will…

Malwarebytes LABS

Search Labs

SUBSCRIBE

NEWS | PRIVACY

‘RockYou2024’: Nearly 10 billion passwords leaked online

Posted: July 8, 2024 by Pieter Arntz

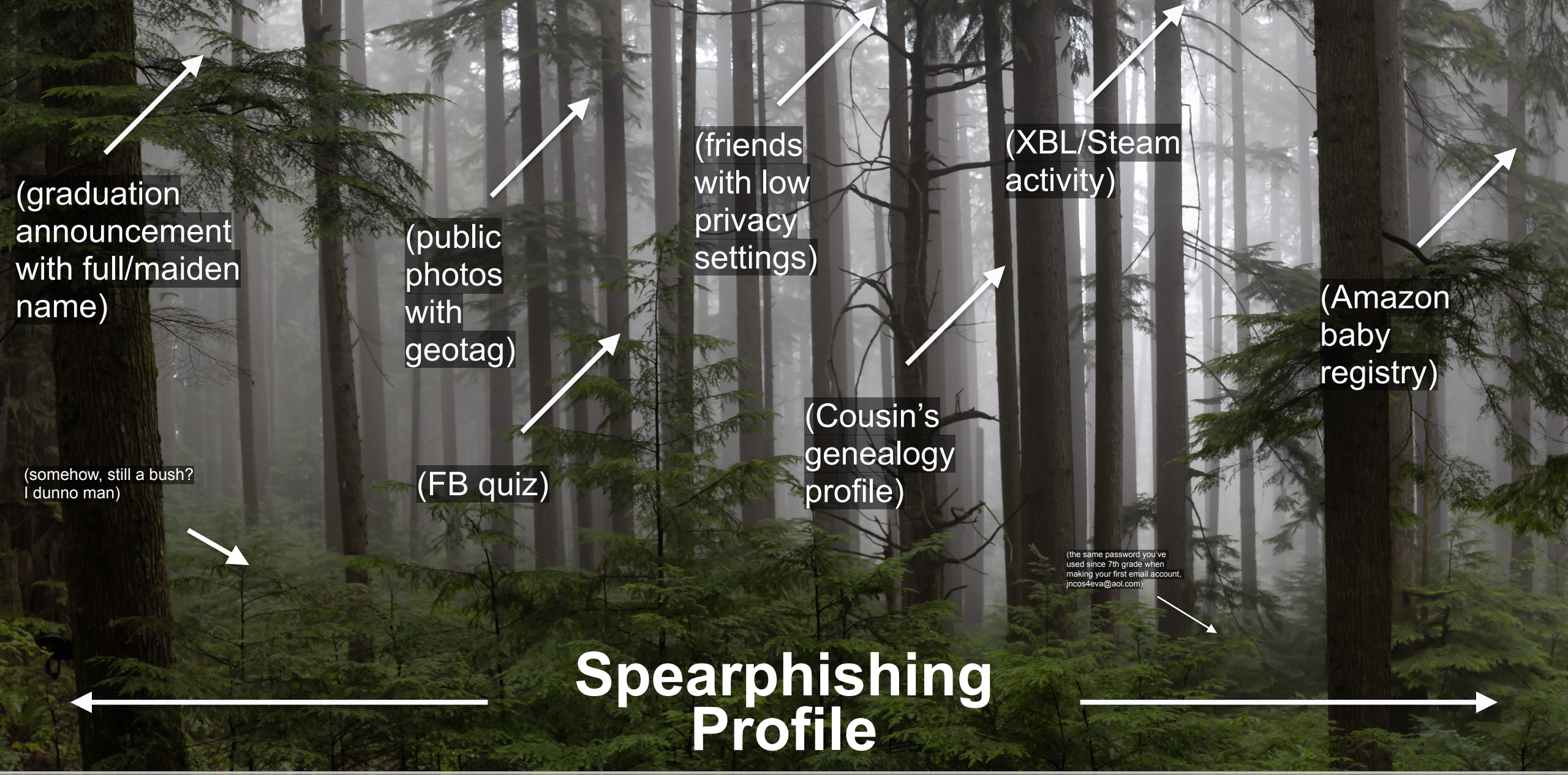
On a popular hacking form, a user has leaked a file that contains 9,948,575,739 unique plaintext passwords. The list appears to be a compilation of passwords that were obtained during several old and more recent data breaches.

The list is referred to as RockYou2024 because of its filename, rockyou.txt.

ABOUT THE AUTHOR

Pieter Arntz
Malware Intelligence Researcher

Was a Microsoft MVP in consumer security for 12 years running. Can speak four languages. Smells of rich mahogany and leather-bound books.

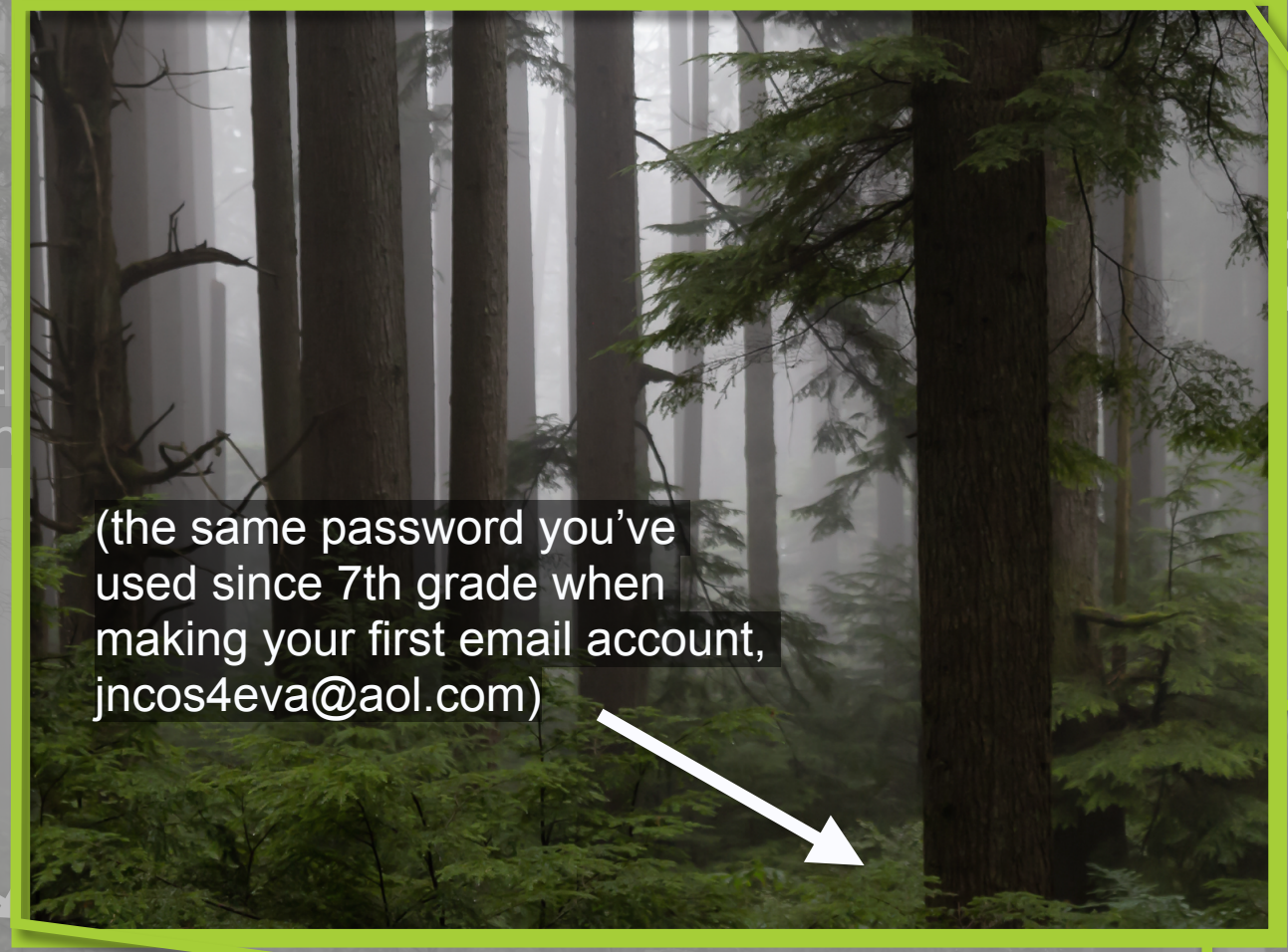

(graduation announcement with full/maiden name)
(public photos with geotag)
(friends with low privacy settings)
(XBL/Steam activity)
(Amazon baby registry)
(somehow, still a bush? I dunno man)
(FB quiz)
(Cousin's genealogy profile)
(the same password you've used since 7th grade when making your first email account, jncos4eva@aol.com)
Spearphishing Profile

(graduation announcement with full/maiden name)

XBL/Steam activity)

(Amazon baby registry)

(somehow, still a bush? I dunno man)

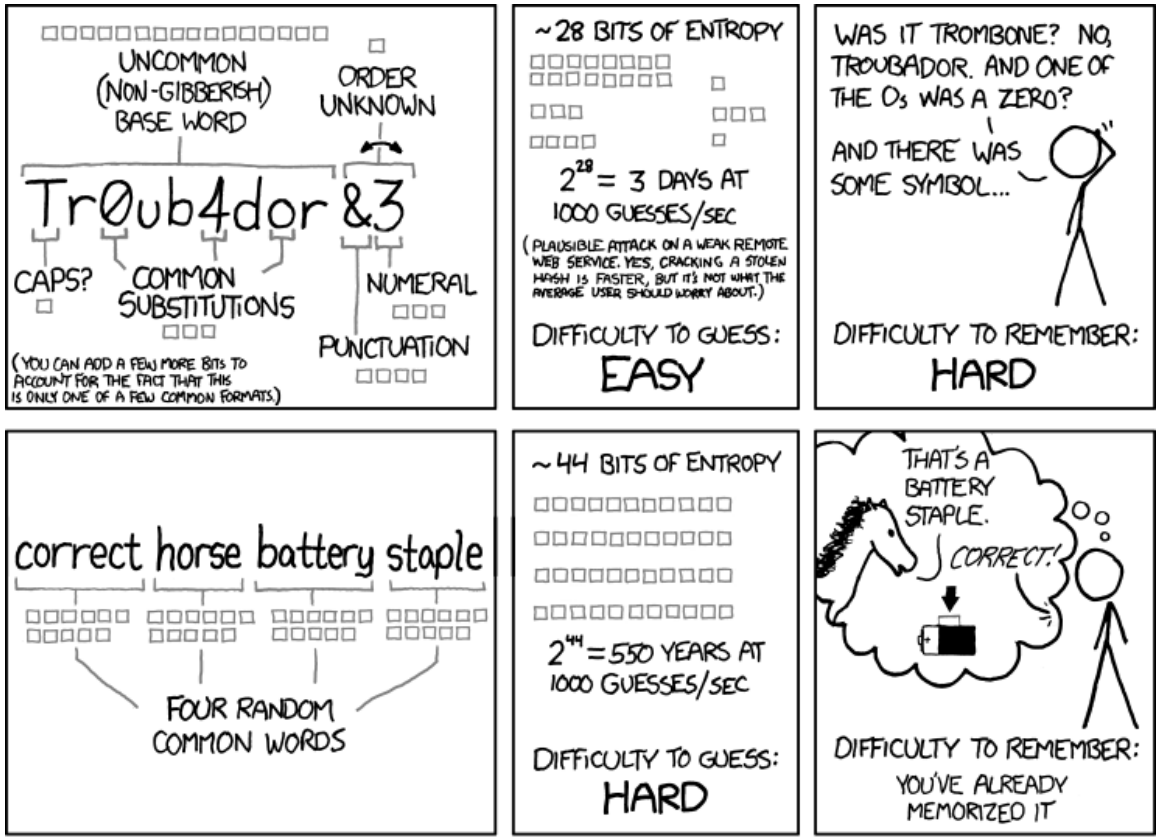


(the same password you've used since 7th grade when making your first email account, jncos4eva@aol.com)

Spearphishing Profile

“My Horse Is My Passport, Verify Me”

- Complex/Random: Good for sufficient entropy, bad for brains
- You’re still not going to remember 168 unique passphrases, anyway, so…
- Just get a password manager
- Also use MFA and passwordless options whenever available


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS:
EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER:
HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS:
HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER:
YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

You Gotta Keep ‘Em Separated

And by “‘em”, of course, I mean “email spheres”

You Gotta Keep ‘Em Separated

And by “‘em”, of course, I mean “email spheres”

- Recovery Email
- High Priority Email
- Social Email
- Low Priority Email

iCloud User Guide

Communities

Search this guide

Table of Contents

Set up and use Hide My Email in iCloud+ on all your devices

You can access Hide My Email on your iPhone, iPad, and Mac, and on iCloud.com if you or someone in your Family Sharing group has an iCloud+ subscription.

For an overview of the feature, see Create unique, random email addresses with Hide My Email and iCloud+.

Note: Make sure you're signed in to the same Apple Account on each device. If you're not signed in to your Apple Account on a device, you won't be able to access Hide My Email on the device.

Set up and use Hide My Email on your iPhone or iPad

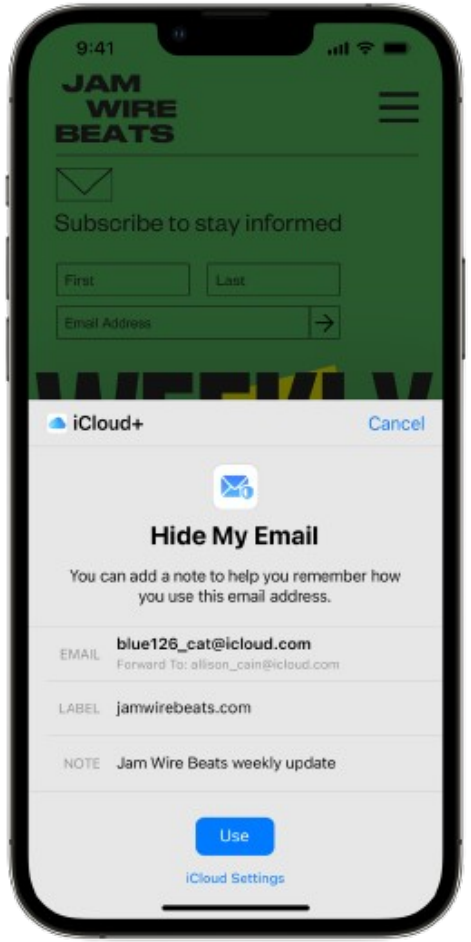
1. On your iPhone or iPad, open Settings.

   Make sure you're signed in to your Apple Account. If you are, you see your name at the top of Settings.

2. To keep your personal email address private, do any of the following:

   - *In Safari:* Open a website, tap in an email field, then tap Hide My Email above the keyboard to generate a new random email address or use one you've already created for the website.
   - *In Mail:* Open a new email window, tap the From field, then choose Hide My Email in the pop-up menu.
   - *In Apple Pay (iOS 17, iPadOS 17, or later):* In the payment sheet, tap Contact, then choose Hide My Email to generate a new email address or use one you've already created for the app or website.

     Note: This option becomes available only when an app or website requests an email from the payment sheet.



PRO-TIP: You Can Just Go On The Internet and Tell Lies!

- Don’t look so shocked, Buster, it’s true
- And it can be good security, too
- Just ask Rebecca Clarke!

PRO-TIP: You Can Just Go On The Internet and Tell Lies!

Rebecca C. Clarke
2779 Rosemont Avenue
Orlando, FL 32810

Curious what **Rebecca** means? Click here to find out!

Mother's maiden name	Cranston
SSN	265-78-XXXX *You should click here to find out if your SSN is online.*
Geo coordinates	28.592549, -81.530326

PHONE

Phone	321-945-8542
Country code	1

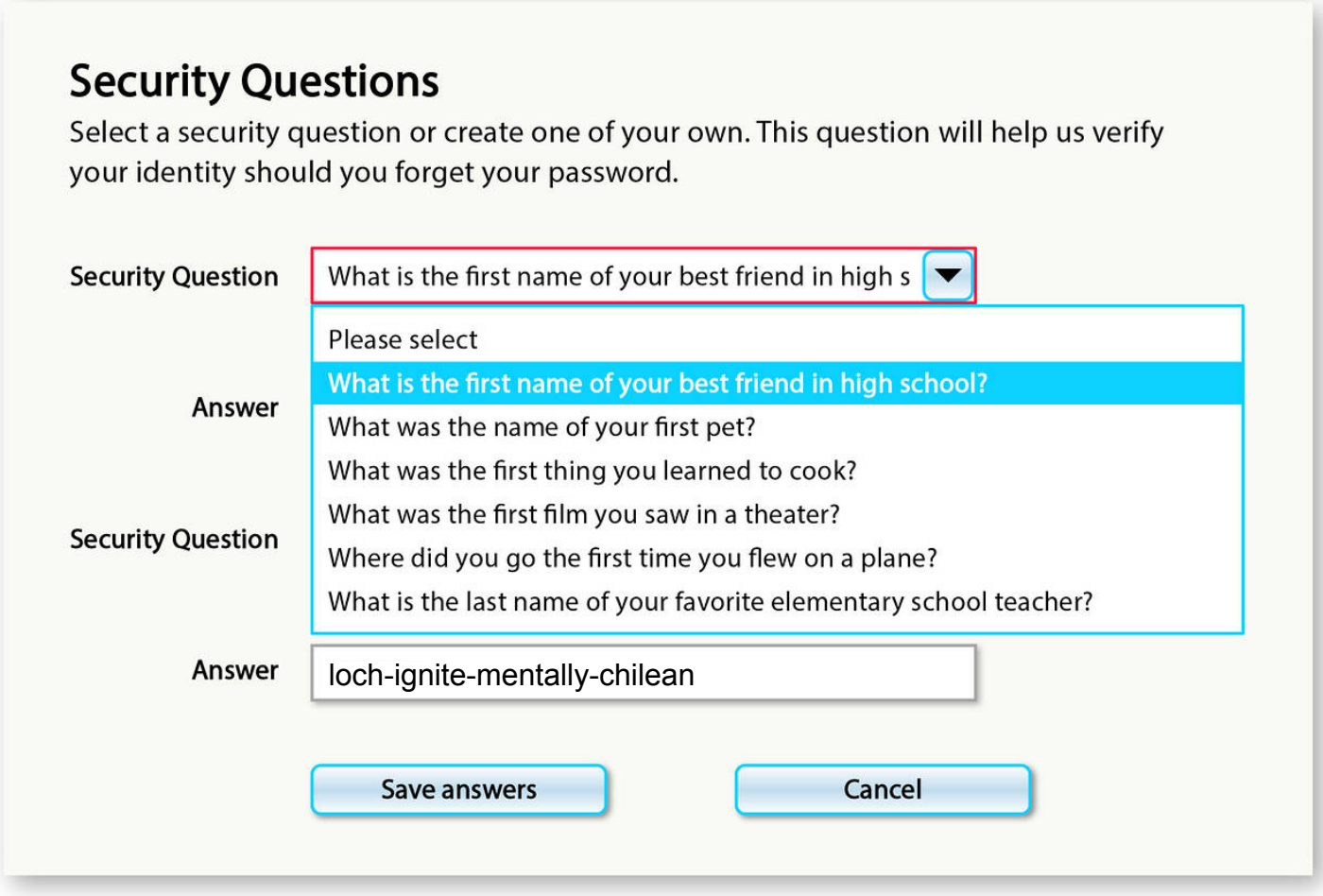
BIRTHDAY

Birthday	September 18, 1989
Age	35 years old
Tropical zodiac	Virgo

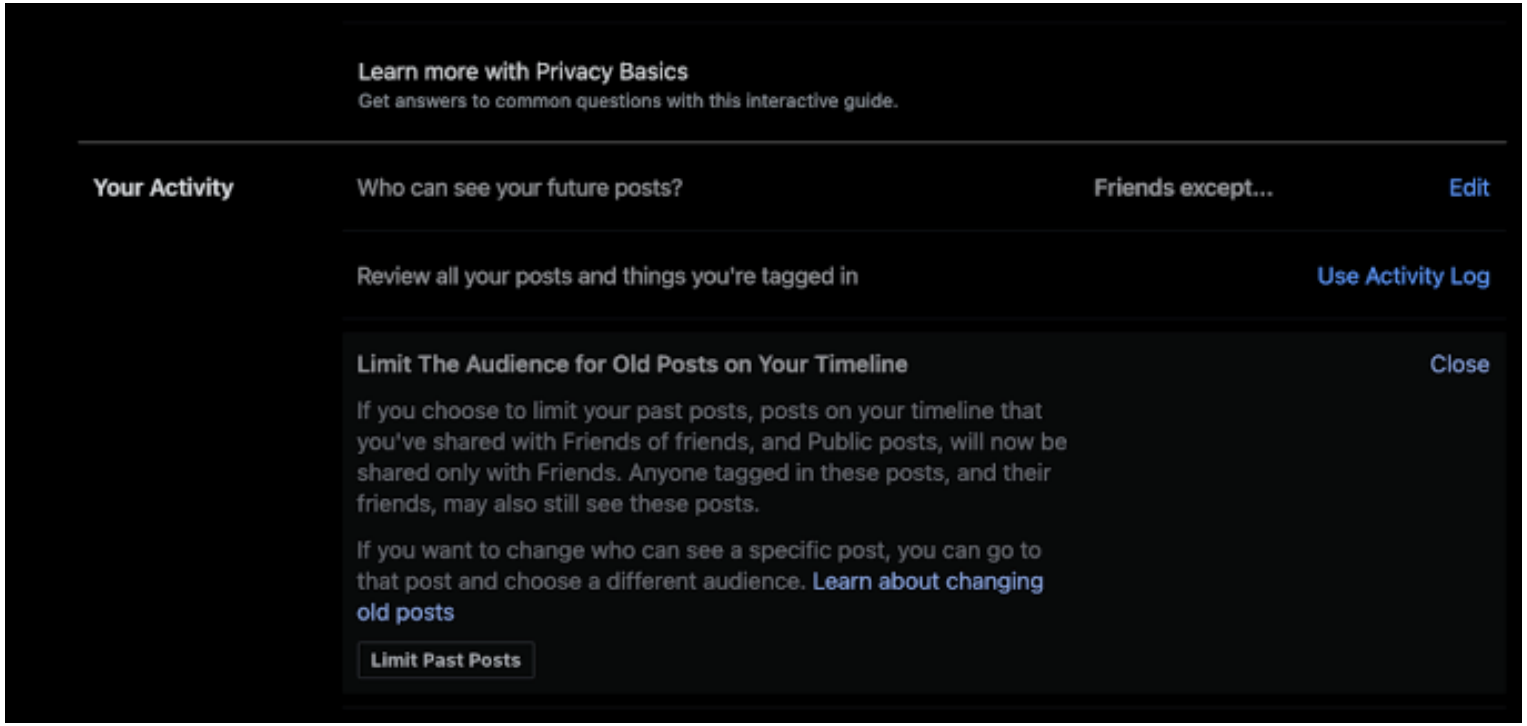
ONLINE

Email Address	RebeccaCClarke@dayrep.com *This is a real email address. Click here to activate it!*
Username	Donsinout
Password	ahyee3AeD0G
Website	sgnol.com

PS: That Goes For Security Questions, Too

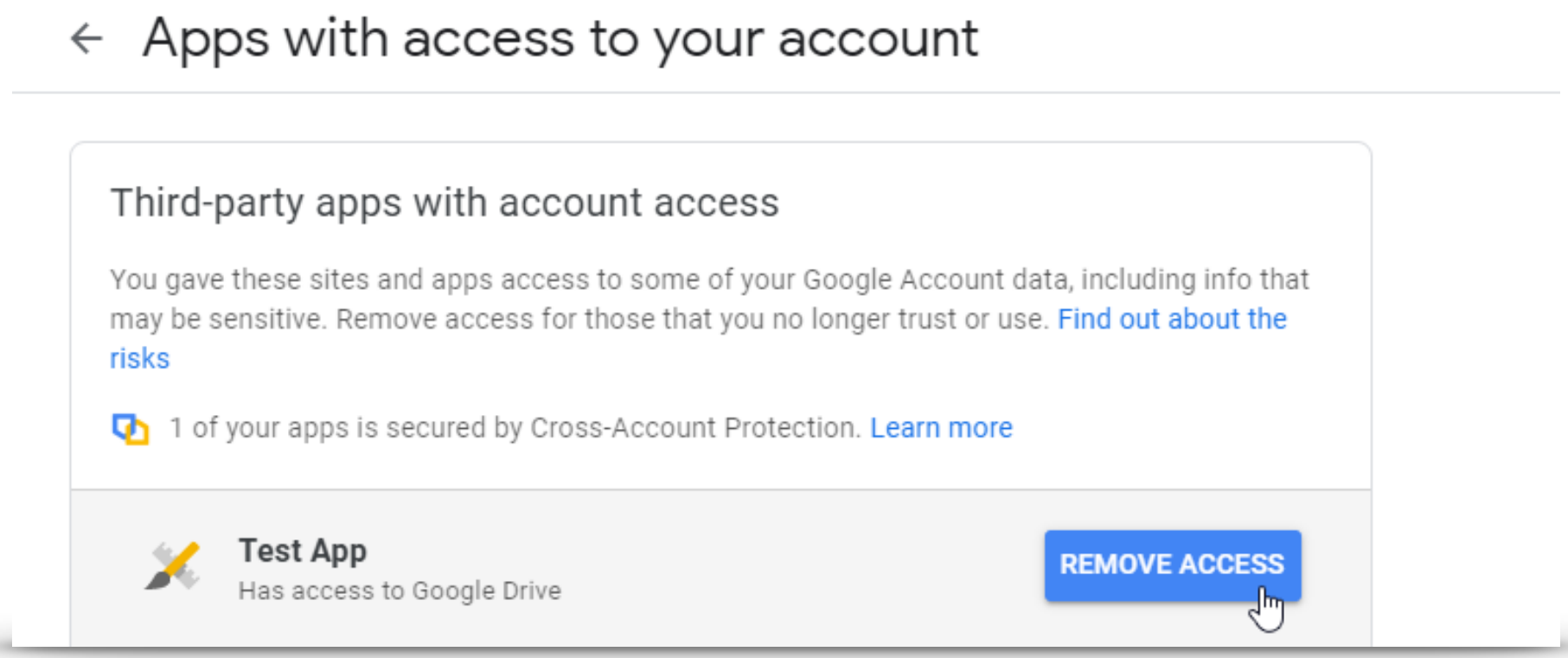

Security Questions
Select a security question or create one of your own. This question will help us verify your identity should you forget your password.
Security Question
What is the first name of your best friend in high s
Please select
What is the first name of your best friend in high school?
What was the name of your first pet?
What was the first thing you learned to cook?
What was the first film you saw in a theater?
Where did you go the first time you flew on a plane?
What is the last name of your favorite elementary school teacher?
Answer
Security Question
Answer
loch-ignite-mentally-chilean
Save answers
Cancel

Good Boundaries Are Good Self-Care

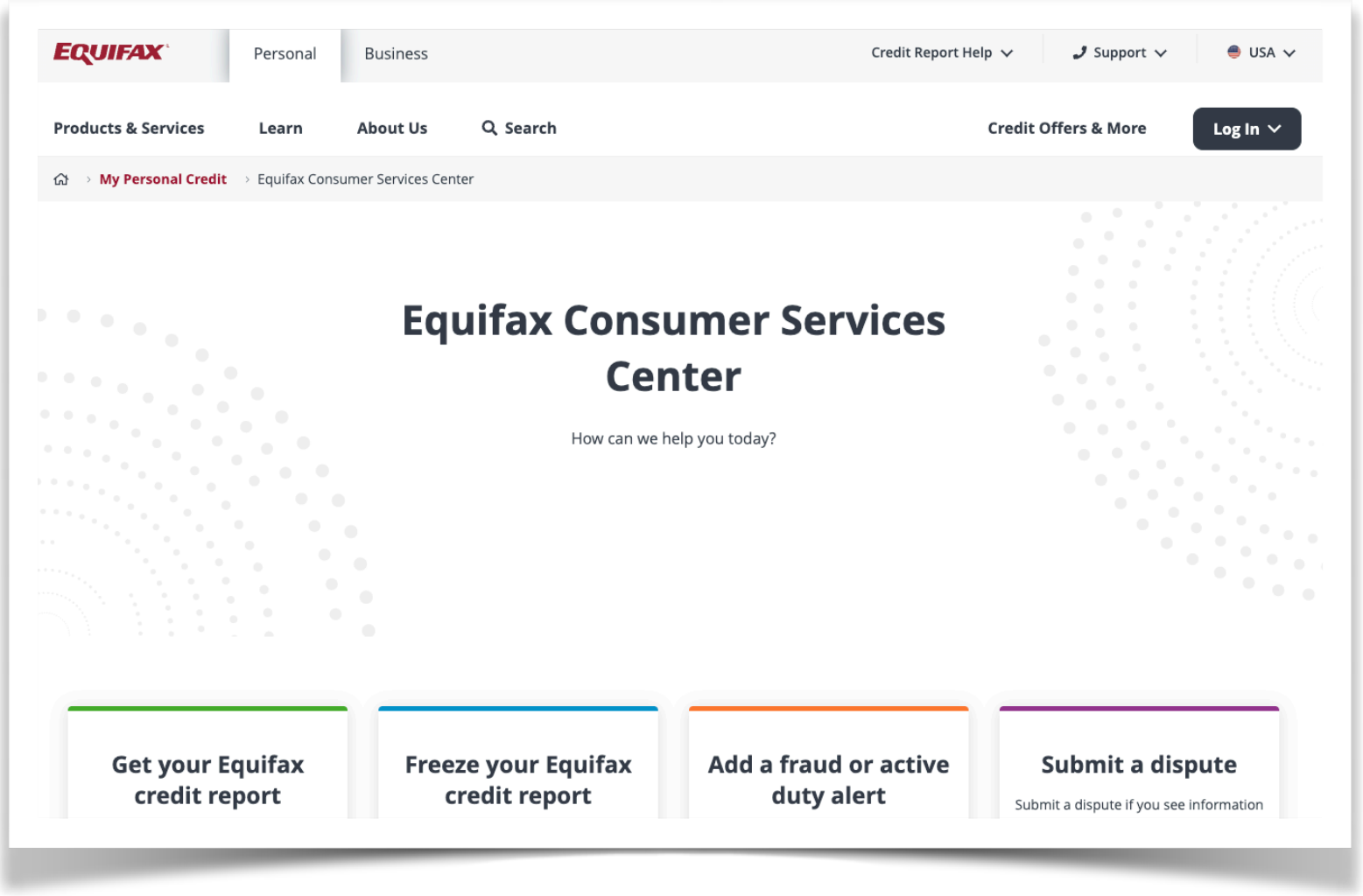

Learn more with Privacy Basics
Get answers to common questions with this interactive guide.
Your Activity
Who can see your future posts?
Friends except...
Edit
Review all your posts and things you're tagged in
Use Activity Log
Limit The Audience for Old Posts on Your Timeline
Close
If you choose to limit your past posts, posts on your timeline that you've shared with Friends of friends, and Public posts, will now be shared only with Friends. Anyone tagged in these posts, and their friends, may also still see these posts.
If you want to change who can see a specific post, you can go to that post and choose a different audience. Learn about changing old posts
Limit Past Posts

- Default Share Settings
- Visibility Settings
- “View As” / Private Browser
- Ad Personalization
- Data Sharing
- Third Party App Account Access

Oops, More Forgotten “Accounts”


Apps with access to your account
Third-party apps with account access
You gave these sites and apps access to some of your Google Account data, including info that may be sensitive. Remove access for those that you no longer trust or use. Find out about the risks
1 of your apps is secured by Cross-Account Protection. Learn more
Test App
Has access to Google Drive
REMOVE ACCESS

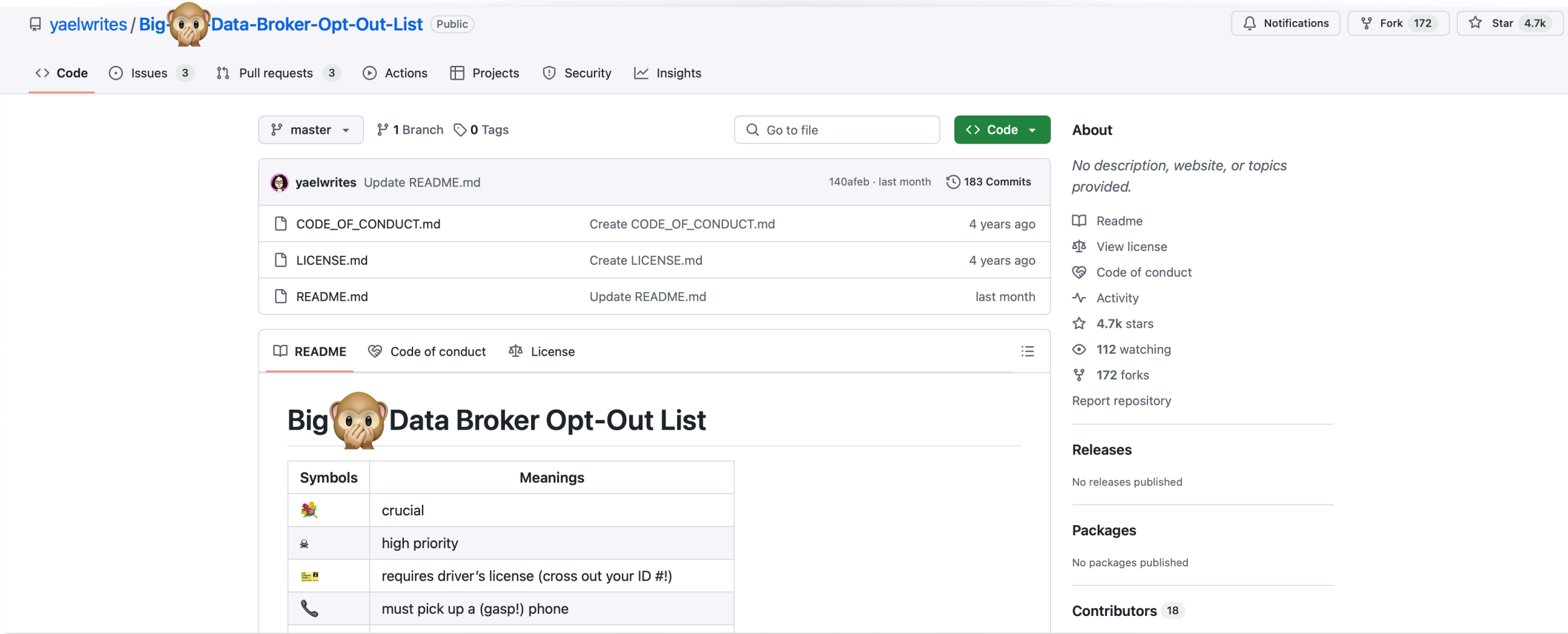
Ice, Ice Baby's Credit Report



- Data Broker Opt-Out
- Cancel Inactive Accounts
- Privacy Removals (where available)

REMOVE

“But How Many Data Brokers Could There Be?”



The Big Ten (not that one)

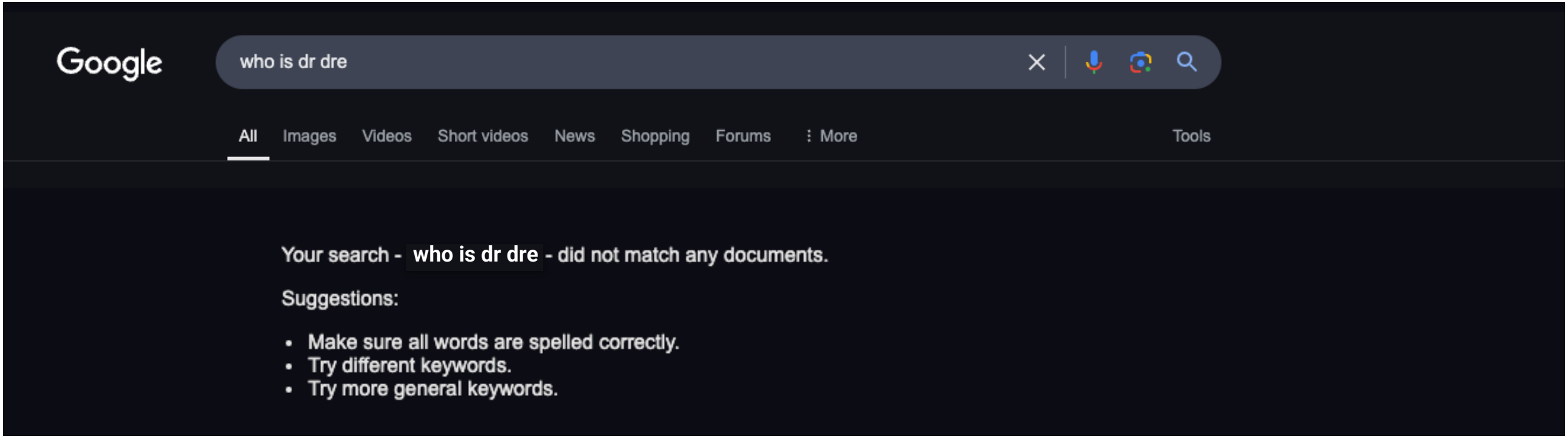
- BeenVerified
- CheckPeople
- ClustrMaps
- Intelius
- MyLife
- Nuwber
- PeopleFinders
- PublicDataUSA
- Radaris
- Spokeo

Digital Spring Cleaning

4shared EASY NO INFO AVAILABLE	500px EASY NO INFO AVAILABLE	9GAG EASY SHOW INFO...	Abload EASY NO INFO AVAILABLE
About.me EASY NO INFO AVAILABLE	Adobe HARD SHOW INFO...	Affero EASY SHOW INFO...	Airbnb EASY NO INFO AVAILABLE
Album Reminder EASY NO INFO AVAILABLE	Alibaba HARD SHOW INFO...	Alvanista EASY SHOW INFO...	Amara EASY SHOW INFO...
Amazon HARD SHOW INFO...	Amazon AWS EASY SHOW INFO...	Animal Crossing Community IMPOSSIBLE SHOW INFO...	AOL / Instant Messenger EASY NO INFO AVAILABLE
App.net EASY NO INFO AVAILABLE	AppFog HARD SHOW INFO...	Argyle Social IMPOSSIBLE SHOW INFO...	ArmorGames EASY NO INFO AVAILABLE
Artsy EASY NO INFO AVAILABLE	Ask.fm EASY NO INFO AVAILABLE	Asos HARD SHOW INFO...	Assembla EASY NO INFO AVAILABLE

Google, You Had ONE Job

How The Internet (Hypothetically) Forgot About Dre



So Now What?

REVIEW

REMOVE

RESTRICT

Hang On, I'll Come In Again.

REVIEW

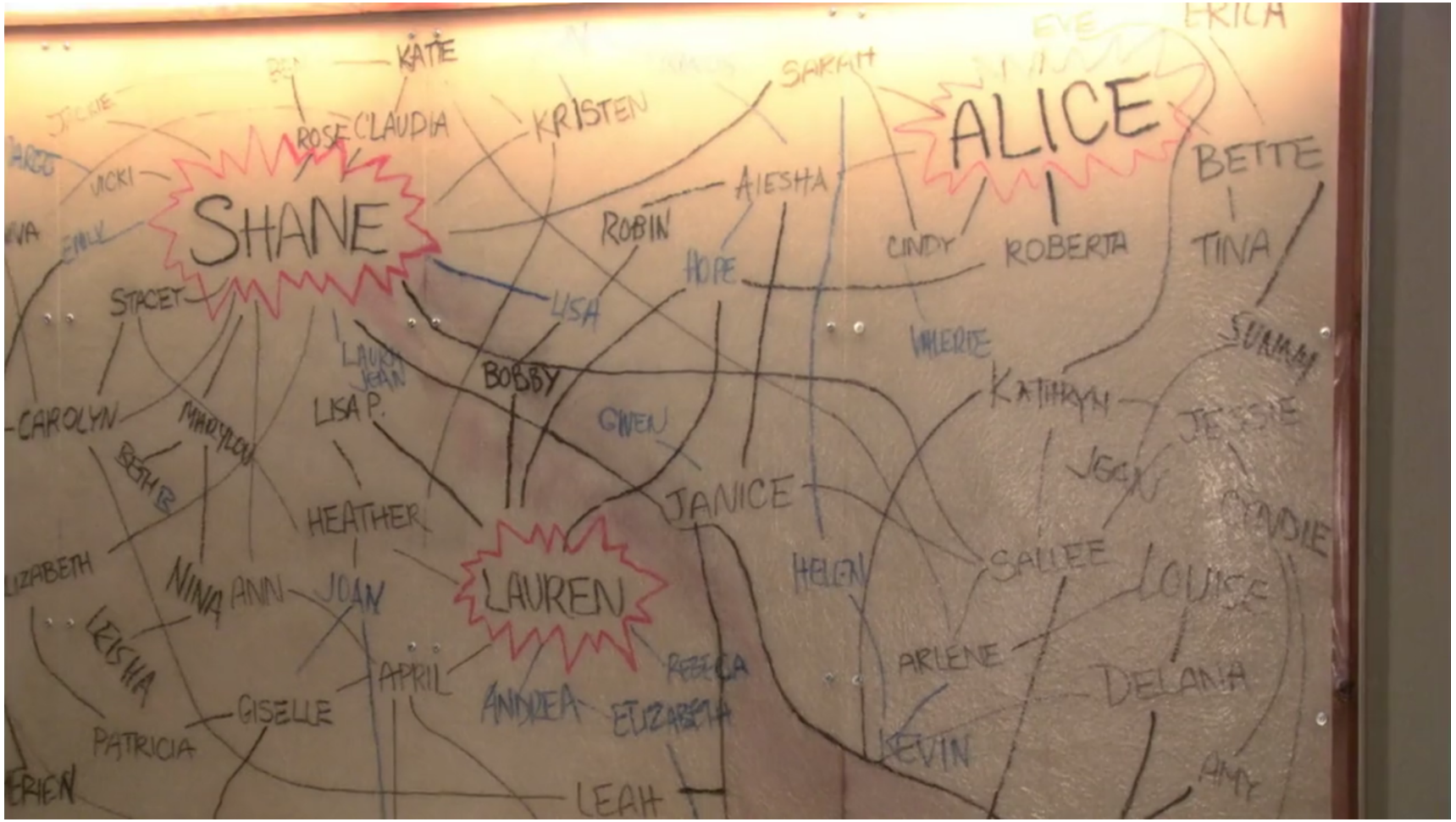
RESTRICT

Blumi

The Adventures of Pete and…

You're Only As Secure As Your Network

Help them help you to help themselves to help… oh, you get the point.



Now It's Your Turn: Put It In Practice!

- **Next week you should:**
  - Download the shared deck
  - Use the resource slides to complete your first self-dox cycle, focusing on the first two levels of review if time-constrained
- **In the first three months following this presentation you should:**
  - Continue working through Levels 3-4, and schedule recurring calendar appointments to repeat this process
- **Within six months you should:**
  - Share what you've learned, whether with your team in a lunch 'n learn, or your family to protect those connected to you as well

Play the exciting TV Game at Home
1 2 3 4 5 6 7 8 9 10 11 12 13 14
1 R E C O R D I A L P H A S E
2 F L I G H T R E E D R A I N
3 B R E A D D E R A W H A L E
4 B L A C K I N G D O M E A L

RSAC™ 2025 Conference

Many Voices.
One Community.

Thank You!

Feedback, Suggestions, or Questions?
Let's Connect!

LinkedIn: linkedin.com/in/zoelindsey
More on Blumira: blumira.com

The following slides are intended to be an interactive resource for your own use while working through the system outlined in this talk

Additional Resources

Guided Exercises

Consumer Reports Security Walkthrough

GCA Security Toolkit for Journalists

How To Use These Slides:

- My goal in this talk was to create an accessible overview teaching what information can be found about us online and what we can do about it.
- The following slides will walk you through each of the Review > Restrict > Remove steps, providing only the resources and instructions

Interactive Guides:

- If you find having a step-by-step walkthrough that you can click as you complete helps, you can take a look at:
    - The GCA Journalist's Toolkit (https://gcatoolkit.org/journalists/) covers some of what we did here, as well as some additional details on securing your laptop/desktop to defend against account takeover
    - I also like Consumer Report's walkthrough (https://securityplanner.consumerreports.org/) which starts by asking you some questions about what devices you use and what you're concerned about

Recommended Reading:

Books:

- *Open Source Intelligence Techniques - Resources For Finding And Analyzing Online Information*, Michael Bazzell, 2022: *https://openlibrary.org/books/OL50061232M/Open_Source_Intelligence_Techniques*
    - Michael has a number of books on OSINT and online privacy which I recommend checking out on his site IntelTechniques as well: *https://inteltechniques.com/links.html*
- *Snoop: What Your Stuff Says About You, Sam Gosling, PhD, 2008: https://archive.org/details/snoopwhatyourstu0000gosl*
- *Systemantics: How Systems Work And Especially How They Fail*, John Gall, 1977: *https://archive.org/details/systemanticshows00gall (not OSINT-specific, but incredibly useful in understanding how humans interact with systems!)*

Articles:

- *"How Apple and Amazon Security Flaws Led to My Epic Hacking" by Mat Honan, Wired, 8/2/2012: https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/*
- *"The Security Mindset", Bruce Schneier, March 2008: https://www.schneier.com/blog/archives/2008/03/the_security_mi_1.html*
- *"SWATting Incidents Tied to ID Theft Sites?" by Brian Krebs, KrebsOnSecurity, 4/17/2023: https://krebsonsecurity.com/2013/04/swatting-incidents-tied-to-id-theft-sites/*

Resources: Review Level 1

- Address History
- Phone Number(s)
- Email(s)
- DOB / SSN
- Search Results

Level 1 - Basic Info

1. Start a list called "Personal Details", for initial web search results and later checking what is discoverable on other data broker sites when requesting removal. Include:

1. Name/DOB
2. Address History
3. Phone Number(s)
4. Email(s)
5. DOB

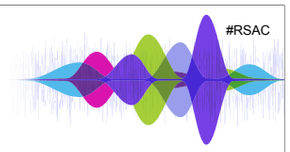
2. Then perform your first round of web searches for initial results, checking both unmodified searches and refined search terms

1. Googledorking Cheatsheet: https://gist.github.com/sundowndev/283efaddbcf896ab405488330d1bbc06

2. Remember that any input you enter will be shared with the search engine (so don't search your SSN!) and if done from your regular account can show in your search history
    1. Most browsers support a "private browsing" or "incognito" option that will not use your authenticated sessions with sites you've already logged into, to avoid adding to your search history
    2. Other search engine options include:
        1. free non-tracking search engines, like DuckDuckGo: https://duckduckgo.com/
        2. paid private search engines, like Kagi: https://kagi.com/
        3. self-hosted (or free public instance) search engines, like SearXNG: https://docs.searxng.org/

3. To automate these search reviews in the future, you can:
    1. Set up Google Alerts for some of your top personal info search terms like your name: https://support.google.com/websearch/answer/4815696?hl=en
        1. Also try your name + city/state, or your name + county as these might turn up more results
    2. Utilize free services like Google's Results About You (https://myactivity.google.com/results-about-you) for automated monitoring
    3. Utilize paid service options like Brightlines (https://www.brightlin.es/) or DeleteMe (https://joindeleteme.com/)

Resources: Review Level 2



- Family Members
- School History
- Work History
- Social Media Profiles
- Usernames/Accounts

Blumira

RSAC 2025 Conference

Level 2 - Primary Connections

1. Update your search term list and complete a second round of searches

1. Start with your immediate and close family members
2. For each, consider how their online activity may affect your risk level or what is being shared about you for consideration during Restrict
3. Repeat for your school and work history, including the companies/institutions as well as close relationships with former classmates and colleagues
4. Then repeat your search process, now specifying “$YOUR_NAME + $YOUR_(SCHOOL, FAMILY MEMBER, COMPANY)_NAME”, and note any results that need attention later

2. Add a new heading for “Critical Accounts” and brainstorm an inventory. These may include:

1. **Financial Accounts:** HR benefits portal, 401k provider, online banking, shopping accounts with payment info attached
2. **Primary Communications Channels**: This includes your primary email(s) as well as accounts that are used as backup for access
    1. (For example, like your cell provider login as many sites will still send an SMS passcode to approve password resets)
3. **Identity Accounts:** If you use another account for single-sign on to multiple sites (like choosing a “sign in with Google/Apple/Facebook/Twitch” option), these should be a priority as well
4. **Healthcare Accounts:** Physician eHealth Portal, insurer’s websites
5. **Professional Tools & Personal Collections:** If you rely on access to do your job, or have built a digital collection like Steam games that has significant value (monetary or sentimental) you likely want to consider it critical
6. If any of these do not currently have long and unique passwords, reviewed privacy settings, and/or strong authentication in place, pause here and go to Review for these accounts before moving on

3. Before moving on to forgotten or discarded accounts, review your social media accounts:

1. Create two more lists (or a new heading) to add alongside the **Personal Details** and **Critical Accounts:** these will be **Restrict** (accounts you’ll review sharing for and retain) and **Remove** (those you no longer wish to keep)
2. Review your privacy and default sharing settings, and visit your profiles from a logged-out browser to see what information is visible.
    1. In particular take a look at
        1. Default post/share settings
        2. Limiting reach on previous posts
        3. Ad personalization, data sharing
        4. Profile searchability/visibility
    2. If you want to restrict these as you go, the NYT Social Media checklists are a great resource as you review the privacy settings for each network you use, and includes most of the popular platforms, and guides you through the labyrinth of privacy settings for each
    3. This deck is a moment-in-time snapshot while the NYT checklists are part of a live document, so I would highly recommend bookmarking it as an evergreen resource for future reviews
3. Inventory forgotten/discarded accounts
    1. Search email
        1. Search for forgotten accounts with common terms: “confirm”, “activate”, “verify”, “subscription”, “password reset”
        2. Refining Gmail searches (syntax may differ depending on provider): https://support.google.com/mail/answer/7190
            1. Example search (without quotes): “subject:{confirm activate (verify your email) (forgot password) subscription (reset password)”
    2. Check for saved credentials on your browser, OS/device, and/or password manager (several options for password managers shared under Restrict
        - Apple:

        - Passwords Help Page: https://support.apple.com/guide/passwords/welcome/mac
        - Safari: *(opens Passwords app)*
    - Google:
        - Password Manager: https://passwords.google.com/
        - Chrome: Settings > Autofill & Passwords
    - Microsoft Edge:
        - Help Page: https://support.microsoft.com/en-us/microsoft-edge/save-or-forget-passwords-in-microsoft-edge-b4beecb0-f2a8-1ca0-f26f-9ec247a3f336
        - Settings > Profiles > Passwords
3. Check an aggregate username/domain search tool to find other places you may have used a given handle or email address to create an account:
    1. InstantUsername (https://instantusername.com) searches a wide variety of sites
    2. NameChk (https://namechk.com) covers less sites, but also checks domains across TLDs

Resources: Review Level 3

- Account Inventory
- Public Records
- Privacy Settings
- Personal Connections
- Search Results

Level 3 - Extended Connections

1. Check for press mentions or inclusion in industry/social publications

1. **Newspapers:**
    1. Google Newspaper Search (https://news.google.com/newspapers) seems to return the most comprehensive results, especially more recently
    2. The Library of Congress Newspaper Directory (https://chroniclingamerica.loc.gov/search/titles/) is another resource, though more useful for pre-2003 records
    3. It's also worth searching local publications on their site directly for the most complete coverage
2. **Yearbooks:**
    1. Ancestry.com has a yearbook search engine covering up to 2016: https://www.ancestry.com/search/collections/1265/
    2. The Internet Archive also has a digitized directory: https://archive.org/details/yearbooks

3. Check for public donations and petition signatures:

1. OpenSecrets (https://www.opensecrets.org/) provides pretty comprehensive results for individual donations

4. Check for reverse image search results on your commonly used profile pictures:

1. Google Search By Image (https://images.google.com/)
2. TinEye (https://tineye.com/)
3. Fuzzy search engines will return more false positives but may find cropped or similar pictures the others miss:
    1. PimEyes (https://pimeyes.com/)
    2. Yandex (https://yandex.com/images/)

5. Check for discoverable information connected to your IP or domain:

- Free IP search engine: shodan.io
    - If you need to know your external IP and ipconfig/ifconfig aren't available/convenient, you can lookup here: https://whatismyipaddress.com/
- WHOIS info:
    - https://lookup.icann.org/en/lookup

Resources: Review Level 4

- Account Inventory
- Public Records
- Privacy Settings
- Personal Connections
- Search Results

Level 4 - Deeper Research

1. Review what data you're sharing with trackers:
- **1. Permissions you've granted to installed mobile apps**
  1. Apple: Settings > Privacy > Permission Manager
  2. Google: Security and Privacy > Privacy Dashboard

2. Be aware of risk when voice/video sharing:
1. Audio- and video-based searches are mostly used currently to find where a file has been shared, but these kinds of personal data can be misused as training data for deepfake imitations. There are evolving defense strategies (several detailed here but for now the best strategy is to be aware of the risk and be mindful of where these media are publicly shared
2. Audio and video files also typically have metadata information that can reveal more about a person's location, equipment/software used, and more

3. Also be aware of the potential risk in your written content through stylometry analysis
1. There are tools available that aim to analyze and reduce the identifiability of text, like anonymouth: https://github.com/spencermwoo/anonymouth

4. For those who do have a higher risk profile, the Gender and Tech Safety Resource further discusses our online footprints (which they call our "digital shadow")
1. I only had time to cover some of the basics on the OSINT side of targeted research, in the interest of being able to provide more generally useful basic defenses that will help the most people
2. There is also additional suggestions on creating and managing segmented email and virtual identities
3. Also detailed are privacy-conscious OS options like
   1. Tails: a portable OS you can run from a thumb drive, and resets to a stock image on each restart
   2. Whonix: a distro built to optimize for anonymity and privacy
   3. Qubes OS: another option using Xen virtualization to compartmentalize data between applications

Resources: Restrict

- Improve Login Security
- Third Party App Access
- Separate Email Channels
- Ad Personalization/Tracking
- Privacy Settings
- Credit Bureau Freeze

RESTRICT

RESTRICT:

1. Improve Login Security

1. Check for compromised passwords
1. HaveIBeenPwned (https://haveibeenpwned.com/) has a searchable index based on email address associated with the breached account
2. Most browsers and password managers now have a “compromised password alert” function now that will notify you if you type or auto-fill credentials previously dumped

2. Get a password manager
1. Many options exist here ranging from
    1. built-in (Apple Passwords) to
    2. free/self-hosted like BitWarden (https://bitwarden.com/) to
    3. paid like 1Password (https://1password.com/)
2. Whichever you choose, make sure your vault password is long, unique, and memorable — your password manager should be a most critical account!

3. Set up strong authentication wherever supported, enabling passkey or MFA options
1. App-based auth is preferable to SMS passcodes, email passcodes shouldn’t be considered a strong MFA method
2. Passwordless/passkey-based authentication lets you use some other method to log in, like approving on a separate device
    1. Most options currently work by scanning a QR code or sending a push notification to approved devices
        1. Google: https://www.google.com/account/about/passkeys/
        2. Apple: https://support.apple.com/guide/iphone/use-passkeys-to-sign-in-to-websites-and-apps-iphf538ea8d0/ios
        3. Microsoft: https://support.microsoft.com/en-us/account-billing/signing-in-with-a-passkey-09a49a86-ca47-406c-8acc-ed0e3c852c6d
        4. More on passkeys: https://www.eff.org/deeplinks/2023/10/what-passkey

2. Restrict Third Party App Access
1. If you have used another account for single sign-on or granted permissions to an external app, see where you’ve used that account to sign in and what permissions are shared. Common platforms:
    1. Google: https://myaccount.google.com/connections
    2. Apple: account.apple.com > Sign-In & Security > Sign In With Apple
    3. Microsoft: https://microsoft.com/consent
    4. Facebook: https://www.facebook.com/settings?tab=applications
    5. Twitter: Settings and Privacy > Security and Account Access > Apps and Sessions

3. Separate Comms Channels:
1. Determine “confidential” levels for your comms. In many cases, setting up 3-4 total accounts can greatly reduce the time needed to keep up on email (centralized on a device logged into all) and reduce how widely accounts

used for sensitive information is shared. These categories are:

1. **Recovery Email**: only used for account verification and resets on most critical accounts
2. **High Priority Email**: This is what you'll use for the most important communications and logins you want to keep track of
    1. (most of your "critical account" list will probably be here)
3. **Social Email:** This is the intentionally-discoverable email you use for networking, public communication
4. **Low Priority Email:** This is distinct from "junk mail", and applies to things like your gym rewards account — you may need to access these periodically, but don't want it clogging up your inbox
    1. When you start contacting data brokers, this is the one you'll use — don't give brokers new info!
5. For throwaway emails you'll only need to check once, I'd just use a disposable service like:
    1. Maildrop: **https://maildrop.cc**
    2. IncognitoMail: **https://incognitomail.co**

2. Another tip to see how/where your data is being shared is to append identifiers on the end of emails, if the provider supports it
    1. So for example, on Gmail, signing up for $NEW_SITE notifications you'd use "myaddress+newsite@domain.tld", and if you see that unique address pop up from another source
    2. Apple provides a similar function for iCloud+ users: https://support.apple.com/guide/iphone/create-and-manage-hide-my-email-addresses-iphcb02e76f7/ios
    3. So do BitWarden (https://bitwarden.com/blog/add-privacy-and-security-using-email-aliases-with-bitwarden/) and DuckDuckGo (https://duckduckgo.com/email/)

3. This comms separation can also be applied to phone contact using services like Google Voice (https://voice.google.com/u/0/about) or another VOIP provider, or seeing if you can inexpensively add a backup line on your cell plan

4. It can also be applied to the digital identity you use itself! Most sites that want your personal info only actually need a fraction of what's shared
    1. Profile pics can be generated by ThisPersonDoesNotExist: https://thispersondoesnotexist.com/
    2. Other details can be generated by FakeNameGenerator: https://www.fakenamegenerator.com/
    3. "Secret questions" can be random strings saved to password manager, or memorable substitutions that aren't actually genuine information about you

4. Ad Personalization/Tracking

1. In most cases, ad personalization options are going to be under the relevant Privacy/Security preferences based on service
2. Mobile devices have their own settings, including notifications what permissions a new app is asking for
3. Apple/Android settings from EFF: https://www.eff.org/deeplinks/2022/05/how-disable-ad-id-tracking-ios-and-android-and-why-you-should-do-it-now
4. Google ad settings: https://myadcenter.google.com/personalizationoff

5. Social Media Privacy Settings

1. **Platform-Specific Settings**
    1. Google: https://safety.google/privacy/
    2. Facebook: https://www.facebook.com/settings?tab=privacy
    3. Instagram: https://help.instagram.com/196883487377501
    4. Twitter: https://x.com/settings/privacy_and_safety
    5. LinkedIn: https://www.linkedin.com/mypreferences/d/categories/profile-visibility
2. The NYT Social Media checklists are a great resource as you review the privacy settings for each network you use, and includes most of the popular platforms, and guides you through the labyrinth of privacy settings for each
    1. This deck is a moment-in-time snapshot while the NYT checklists are part of a live document, so I would highly recommend bookmarking it as an evergreen resource for future reviews
3. Common settings to check:
    1. Default share / prior post reach
    2. Search / visibility settings
    3. "View As" to see if share circles are functioning as defined (otherwise checking in private browser)
    4. Data Sharing / Do Not Track settings
    5. Third Party Account Access (detailed above)
4. Location setting (Geolocation):
    1. Check geolocation sharing settings on your most-used capture devices for photos/videos
        1. Android: https://support.google.com/photos/answer/9921876?hl=en
        2. Apple: https://support.apple.com/guide/personal-safety/manage-location-metadata-in-photos-ips0d7a5df82/web
    2. More info on geolocation tools, tactics, and preventative measures from SANS: https://www.sans.org/blog/geolocation-resources-for-osint-investigations/

6. Credit Freeze

1. **Equifax:** https://www.equifax.com/personal/credit-report-services/
2. **Experian:** https://www.experian.com/freeze/center.html#content-01
3. **TransUnion:** https://service.transunion.com/dss/orderStep1_form.page

7. General Best Practices We Haven't Talked About Yet

1. **Use different, generic usernames without identifying info**
    1. (for example, avoid BandILike89… if you're a fan of Band and were born in 1989)
2. **Lock your phone / computer with a password/PIN (or even better, U2F/biometric!)**
    1. If someone finds your phone unlocked, it will save them a lot of time researching
3. **Update your browser and devices**
    1. Most malware exploits vulnerabilities that have received updates from the developer, but continue to succeed because of out-of-date devices
    2. Keeping your software and devices updated is one of the best steps to prevent a breach

Resources: Remove

- Data Broker Opt-Out
- Cancel Inactive Accounts
- Privacy Removals (where available)

REMOVE

REMOVE

Remember: Removal is an ongoing process! You probably didn't create every account on the same data, and it takes a whole industry of data brokers to parcel and repackage our personal information, so think of this as something you do in short, repeatable sessions rather than a single all-day (or days-long) endurance exercise

1. Data Brokers:

1. The **Big A(hh) Data Broker List** (**https://github.com/yaelwrites/Big-Ass-Data-Broker-Opt-Out-List**) is an updating source that helpfully splits brokers into categories of severity
    1. Try to tackle the Top 10 in your first session, and then move on to the others
    2. DO NOT give brokers new information! Use your low-priority account or a unique alias, as well as VOIP if something like a phone is required
2. I would be remiss to not include the **IntelTechniques Workbook** (**https://inteltechniques.com/data/workbook.pdf**) which makes up for its static list by being as exhaustive as possible. Some of these brokers are no more (or have been acquired/rebranded), but there are also brokers listed here I haven't found on any other list

2. Cancel Abandoned or Unwanted Accounts:

1. JustDeleteMe (https://backgroundchecks.org/justdeleteme/): online account cancellation details
2. AccountKiller (https://www.accountkiller.com/en/home): additional offline cancellation processes
3. Do a backup of your data before canceling, and make sure you've checked that you've updated any third party sharing or ad metric settings first!

3. Request Search Engine Privacy Removals for Unwanted or Inaccurate Results:

1. Much of this is region- rather than service-specific, as many platforms will limit removal requests and other privacy requirements in jurisdictions that don't enforce those controls. So if you're in…
    1. The EU, you can check GDPR (https://gdpr-info.eu/)
    2. California, you can check your rights under CCPA (https://oag.ca.gov/privacy/ccpa)
    3. Germany, take a look at the Bundesdatenschutzgesetz: https://www.bmi.bund.de/EN/topics/it-internet-policy/data-protection/data-protection-node.html
        1. (this goes in Resources notes so I don't have to try and pronounce it)
2. Some search engine-specific results to check:
    1. Google: https://support.google.com/websearch/answer/12719076?hl=en
    2. Microsoft: https://www.microsoft.com/en-us/privacy/privacy-support-requests (under "Make A Request")
    3. Yahoo: (https://help.yahoo.com/kb/SLN4374.html (TL;DR: they say "don't share it if you don't want us to index it)